§1.2 Cyclic semigroups

Recall Mehmet defined for $s \in S$ a semigroup the cyclic subsemigroup $\langle s \rangle = \{s, s^2, s^3, \ldots\}$

(if $S$ was a monoid, the submonoid gen'd by $s$
would be $\{s^0, s^1, s^2, s^3, \ldots\}$ )

For $s \in S$ a finite semigroup, we defined

index $c$: smallest $c \geq 1$ such that $s^{c+d} = s^c$ for some $d$

period $d$: smallest $d \geq 1$ such that $s^{c+d} = s^c$ for some $c$

EXAMPLE

$\xrightarrow{s} s^2 \xrightarrow{s} s^3 \xrightarrow{s} s^4 \xrightarrow{s} s^5 \xrightarrow{s} s^6 \xrightarrow{s} s^7$

index $c = 7$
period $d = 5$
We proved...

**Prop 1.1, Cor 1.2, Cor 1.4:**
For every \( s \in S \) a finite semigroup, \( \langle s \rangle = \{ s, s^2, s^3, \ldots \} \)
- contains a unique idempotent \( e^2 = e \), namely \( e = s^{\omega} \) where \( \omega \equiv 0 \mod d \) and \( \omega \geq c \).
- Furthermore, \( e \) is the identity element for \( C := \{ s^0, s^{c_1}, s^{c_2}, \ldots \} \) which is a subgroup of \( S \).
- \( C \cong \mathbb{Z}/d\mathbb{Z} \) is a cyclic group generated by \( s^{c_1} = s^{c_3} \cdot s \)

---

**Example**

\( s \rightarrow s^2 \rightarrow s^3 \rightarrow s^4 \rightarrow s^5 \rightarrow s^6 \rightarrow s^7 \)

- Index \( c = 7 \)
- Period \( d = 5 \)
- \( \omega = 10 \equiv 0 \mod 5 \)

\( C \cong \mathbb{Z}/5\mathbb{Z} \)
Remark 1.3
If \( n = 18 \) then \( \forall s \in S \), more concretely this idempotent \( e = s^{n!} = s^n \)
since both \( e, d \leq |S| = n \) \[ \Rightarrow \begin{cases} n! \geq n \geq c \\ n! \equiv 0 \mod d \end{cases} \]

**DEF'N:** \( E(S) := \{ \text{idempotents } e^2 = e \text{ in } S \} \)

Lemma 1.6 If \( S \xrightarrow{\Phi} T \) is a surjective morphism of finite semigroups \( S, T \), then \( \Phi( E(S) ) = E(T) \).

**proof:** \( \Phi(E(S)) \subseteq E(T) \) since \( e^2 = e \Rightarrow \Phi(e^2) = \Phi(e) \Rightarrow \Phi(e)^2 \)

For surjectivity \( E(S) \xrightarrow{\Phi} E(T) \), given \( e \in E(T) \), note \( \Phi^{-1}(e) \) is nonempty and a finite subsemigroup of \( S \), so it contains an idempotent \( e' \in E(S) \).
§1.3 Ideal structure and Green's relations

M a finite monoid throughout this discussion.

DEF'N: A nonempty subset $I \subseteq M$ is a ...

- left ideal if $MI \subseteq I$
- right ideal if $IM \subseteq I$
- (2-sided) ideal if $MIM \subseteq I$

All are subsemigroups, so contain idempotents.

Any two ideals $I, J$ both contain another ideal

$IJ := \{ij : i \in I, j \in J\} \subseteq I, J$

so a finite monoid $M$ has a ! minimal ideal
(namely $I_1I_2...I_n$ where $I_1, ..., I_n$ are all of its ideals)
Example

1. \( M = M_n(k) = \{ n \times n \text{ matrices over a field } k \} \)
   has its only ideals \( I_r = \{ \text{matrices of rank } \leq r \} \)
   unique minimal ideal \( I_0 \subset I_1 \subset \cdots \subset I_{n-1} \subset I_n \)
   \[
   \begin{bmatrix}
   I_r & 0 \\
   0 & 0
   \end{bmatrix}
   \]
   \( M_n(k) \)

   Right ideals are of form \( \{ \text{matrices } A \text{ with } \text{im}(A) \leq V \} \)
   Left ideals are of form \( \{ \text{matrices } A \text{ with } \text{ker}(A) \supseteq U \} \)
   for any choices of subspaces \( U, V \subset k^n \)

   Exercise: Check me using \( \text{im}(AB) \leq \text{im}(A) \), \( \text{ker}(BA) \supseteq \text{ker}(A) \).

2. For \( m \in M \), \( MM = \) principal left ideal,
   \( mM = \) right ideal,
   \( MmM = \) (2-sided) ideal
   generated by \( m \).

3. \( I(m) := \{ s \in M : m \notin MsM \} \) is an ideal
   (if it's nonempty) as \( m \notin MsM \Rightarrow m \notin MaM \subset MsM \)
   \( I(m) = \emptyset \Leftrightarrow m \in \) minimal ideal
   e.g. in \( M_n(k) \),
   \( I(A) = \{ B : \text{rank} B < \text{rank} A \} \)
**DEF’N:** Green’s relations (J.A. Green 1951)

Say \( m_1 \mathrel{J} m_2 \) if \( Mm_1 M = Mm_2 M \) (same principal ideal)

\( m_1 \mathrel{L} m_2 \) if \( Mm_1 = Mm_2 \) (same principal left ideal)

\( m_1 \mathrel{R} m_2 \) if \( m_1 M = m_2 M \) (same principal right ideal)

---

**EXAMPLES**

1) For \( M = M_n(k) \) nxn matrices

\[ A \mathrel{J} B \iff \text{rank} A = \text{rank} B \]

(so \( B = PAQ \) with \( P, Q \in \text{Gl}_n(k) \))

\[ A \mathrel{L} B \iff A, B \text{ are row-equivalent} \]

(so \( B = PA \))

\[ A \mathrel{Q} B \iff A, B \text{ are column-equivalent} \]

(so \( B = AQ \))
(2) For $T_n := \{ \text{all self-maps } f : \{1,2, \ldots, n\} \to \{1,2, \ldots, n\} \}$ under composition $f \circ g$

**Full transformation monoid of degree $n$**

$f \sim g$ if $f, g$ have same partition of source into fibers $f(i), g(i)$

$f \sim g$ since $f = h \circ g$

$g = h \circ f$

$f \sim g$ if $\text{im}(f) = \text{im}(g)$

$f \sim g$ since $g = f \circ h$

and can similarly find an $h'$ with $f = g \circ h'$

$f \sim g$ if $\#\text{im}(f) = \#\text{im}(g)$

$f \sim g$ if $\Rightarrow T_n$ has ideals

$I_1 \subset I_2 \subset \ldots \subset I_n$

$\text{constantly [maps]}$

$\Rightarrow T_n$

$I_r = \{ f : \#\text{im}(f) \leq r \}$
DEF'N  M is $\mathcal{R}$-trivial if $m_1 M = m_2 M \Rightarrow m_1 = m_2$

$\mathcal{L}$-trivial if $M m_1 = M m_2 \Rightarrow m_1 = m_2$

$\mathcal{J}$-trivial if $M m_1 M = M m_2 M \Rightarrow m_1 = m_2$

i.e. the various relations $\mathcal{R}, \mathcal{L}, \mathcal{J}$ are just equality

NOTE

$\mathcal{J}$-trivial $\Rightarrow$ $\mathcal{R}$- and $\mathcal{L}$-trivial

![Diagram of various monoids and groups]  

From Denton, Hivert, Schilling, Thiery 2011:

Note groups are not $\mathcal{J, R, L}$-trivial: $g R g', g L g', g J g'$.
Green's relations are compatible with restricting to submonoids $eMe$, $e$ idempotent.

**LEMMA 1.7**: For an idempotent $e \in E(M)$ and $m_1, m_2 \in eMe$, one has

$$m_1 \equiv m_2 \text{ in } M \iff m_1 \equiv m_2 \text{ in } eMe$$

and same for $L$, $J$.

**proof**: Do the proof for $J$; for $R$, $L$ is similar.

$$eMe \cdot m_1 \cdot eMe = eMe \cdot m_2 \cdot eMe$$

$$\iff \exists a, b, c, d \in eMe \text{ with } m_1 = am_2b$$

$$m_2 = cm_1d$$

$$\Rightarrow Mm_1M = Mm_2M.$$

Conversely, if $Mm_1M = Mm_2M$ then

$$eMe \cdot m_1 \cdot eMe = eMm_1Me = eMm_2Me = eMe \cdot m_2 \cdot eMe$$
**M-sets**

In studying $L, \mathbb{R}, J$, it helps to have the notion of $M$ (left) acting on a set $X$:

A map $M \times X \rightarrow X$

$(m, x) \rightarrow mx$

with $1_x = x \forall x \in X$

$m_1(m_2 x) = (m_1 m_2) x$

Call it a **faithful action** if $m x = m' x \forall x \in X$

$\Rightarrow m = m'$ in $M$

---

A map $X \xrightarrow{\varphi} Y$ is **$M$-equivariant** if

$\varphi(mx) = m \varphi(x) \forall m \in M \forall x \in X$

and an **isomorphism** $X \cong Y$ of $M$-sets if bijective.

$\text{Hom}_M(X, Y) = \{ \text{M-equivariant } X \xrightarrow{\varphi} Y \}$
**Prop 1.8**: For an $M$-set $X$ and $e,e \in E(M)$

(c) one has a bijection $\text{Hom}_M(M,e_X) \cong e_X^X \quad \varphi \mapsto \varphi(e)$.

\[
\begin{align*}
\text{Take } X &= M \\
\text{(iii)} \quad \text{End}_M(M,e) &= (eM)_e^{op} \quad \text{as monoids}
\end{align*}
\]

\[
\begin{align*}
\text{apply } A &\mapsto A^\times \\
\text{monoid } \quad \text{group of units}
\end{align*}
\]

\[
\begin{align*}
\text{(iv)} \quad \text{Aut}_M(M,e) &= (G_e)_e^{op} \quad \text{as groups}
\end{align*}
\]

where $G_e := \text{group of units in } eM$. 

\[
\begin{align*}
\text{PROP} \quad 1.8: \quad &\text{For an } M\text{-set } X \text{ and } e \in E(M) \\
\text{c) one has a bijection } \text{Hom}_M(M,e_X) \cong e_X^X \quad \varphi \mapsto \varphi(e). \\
\text{Take } X = M \\
\text{(iii)} \quad \text{End}_M(M,e) &= (eM)_e^{op} \quad \text{as monoids} \\
\text{apply } A &\mapsto A^\times \\
\text{monoid } \quad \text{group of units} \\
\text{(iv)} \quad \text{Aut}_M(M,e) &= (G_e)_e^{op} \quad \text{as groups} \\
\text{where } G_e := \text{group of units in } eM.
\end{align*}
\]
Prop 1.8: For an M-semi X and e ∈ E(M)

(i) one has a bijection \( \text{Hom}_M(Me, X) \cong eX \)

\( \phi \mapsto \phi(e) \).

(ii) \( \text{End}_M(Me) \cong (eMe)^\circ \) as monoids

(iii) \( \text{Aut}_M(Me) \cong (Ge)^\circ \) as groups

where \( Ge := \text{group of units in } eMe \).

Proof: If \( \phi \in \text{Hom}_M(Me, X) \), then \( \phi(e) \in eX \)

since \( \phi(e) = \phi(e^2) = e\phi(e) \), and \( \phi(e) \) determines \( \phi \)

via \( \phi(me) = m\phi(e) \). The inverse bijection

\[
\text{Hom}_M(Me, X) \cong eX \\
\phi(me) \mapsto \phi(e)
\]

Then (ii) is (i) taking \( X = Me \), noting \( (\psi \circ \phi)(e) = \psi(\phi(e)) \)

\[= \psi(\phi(e)e) = \phi(e)\psi(e) \).

Lastly (ii) \( \Rightarrow \) (iii) applying \[\text{monoid} \rightarrow \text{group of units} \]
REMARK 1.9: If one doesn’t like the “op”s, 
\[(ii) \text{End}_\text{M}(\text{Me}) \cong (\text{eMe})^\circ \]
says eMe acts on the right of Me 
via M-set maps, and gives all such maps.

Likewise, \[(iii) \text{Aut}_\text{M}(\text{Me}) \cong (\text{Ge})^\circ \]
says Ge acts (as a group) on the right of Me.

PROP 1.10:
Ge (right-)acts freely on Le = \(\mathcal{L}\)-class of e 
= generators of Me 
(and (left-)acts freely on Re = \(\mathcal{R}\)-class of e).

proof: For action, if meLe and ge Ge \((= (\text{eMe})^x)\), 
want mg eLe , that is Me \(\cong\) Mmg:

\[\ge: g = ege \Rightarrow Mmg = M\text{mege} \subseteq M\text{e} \]

\[\le: meLe \Rightarrow \exists y \in M \text{ with } e = ym \]
so \(e = \tilde{g}^t \tilde{g} = \tilde{g}^t \text{eg} = \tilde{g}^t \text{ymg} \)
and Me = M\text{yymg} \subseteq Mmg
For freeness, using same $m, g, y$ as above
if $mg = m$ then $g = eg = ymg = ym = e$.  

\[ \text{EXAMPLE} \quad \text{When } M = M_n(k) = \text{n}\times\text{n matrices,} \]

\[ \text{a typical idempotent } e \in E(M) \text{ is} \]

\[ e = \begin{bmatrix} V_1 & V_2 \\ V_2 & O \end{bmatrix} \]

where $V = k^n = V_1 \oplus V_2$

\[ \text{having } eMe = \left\{ \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix} : A \in M_r(k) \right\} \]

\[ G_e = (eMe)^x = \left\{ \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix} : A \in \text{GL}_r(k) \right\} \]

and the generators $L_e$ of $Me$ =\[ \left\{ \begin{bmatrix} A & 0 \\ B & 0 \end{bmatrix} \right\} \]

have lin. indep. 1st $r$ columns, carrying a

\[ \text{free action of } G_e \text{ on the right.} \]

\[ \left[ G_e \text{-orbits} \leftrightarrow \text{r-dim'l subspaces of } k^n \quad \text{on } L_e \text{ given by col space of } \begin{bmatrix} A & 0 \\ B & 0 \end{bmatrix} \right] \]
Now can relate $M$-set structure for $Me$, $eM$ to Green's $J$.

**THM 1.11** For idempotents $e, f \in \mathcal{E}(M)$, TFAE:

(i) $Me \cong Mf$ as (left-) $M$-sets

(ii) $eM \cong fM$ as (right-) $M$-sets

(iii) $\exists g, h \in M$ with $e = ab$

(iv) $\exists x, x' \in M$ with $x x' x' = x$ and $e = x' x$

(v) $MeM = MfM$ (i.e. $eJf$.)

---

**Note an immediate --**

**COROLLARY 1.12** When idempotents $e, f \in \mathcal{E}(M)$ have $eJf$, then $eMe \cong fMf$ as monoids, and $G_e \cong G_f$ as groups.

(since $eMe \cong \text{End}_M(eM)$ and $G_e = (eMe)^*$ )
**Example:** Recall for $M = M_n(k)$

$$ef \iff \text{rank}(e) = \text{rank}(f)$$

So if we have idempotents $e, f \in \text{End}(M)$ with $ef \neq 0$ then one can write

$$V = k^n = \text{im}(e) \oplus \ker(e)$$

If $e$ is idempotent, then $e = \text{im}(e) \oplus \ker(e)$.

Then $e = ab = \text{im} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}_{\ker}$

$$f = ba = \text{im} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}_{\ker}$$
Theorem 1.11: For idempotents $e, f \in E(M)$, TFAE:

(i) $M e \cong M f$ as (left-) $M$-sets

(ii) $e M \cong f M$ as (right-) $M$-sets

(iii) $\exists g \in E(M)$ with $e = ab$

(iv) $\exists x, x' \in E(M)$ with $xx'x = x$ and $e = x'x$

(v) $MeM = MfM$ (i.e. $e \not\subseteq f$)

Proof Strategy:

Show (i) \implies (iv) (and replacing (i) by (ii) follows by left-right symmetry)
(i) \( Me \cong Mf \) as \((\text{left-})\) \(M\)-sets

\[ \Downarrow \]

(iv) \( \exists x, x' \in M \) with \( xx' = x \) and \( e = x'x \)
\[ x'x' = x' \quad f = xx' \]

---

Given inverse \(M\)-set isomorphisms \( Me \xrightarrow{\psi} Mf \),

\[
\begin{align*}
\text{let } x' & := \psi(e) \\
x & := \psi(f)
\end{align*}
\]

\[
\begin{bmatrix}
\psi(ee) = e\psi(e) & e \in Mf \\
\psi(ff) = f\psi(f) & f \in Mf
\end{bmatrix}
\]

and check
\[ x'x = x'\psi(f) = \psi(x'f) = \psi(x') = \psi(\psi(e)) = e \]

(and similarly for \( xx' = f \).)

Also \( x'x x' = e x' = x' \quad \text{since } x' \in eMf \)

and \( xx'x = fx = x \quad \text{since } x \in fMe \)
(i) $\text{Me} \cong \text{Mf}$ as (left-) $\text{M}$-sets

(ii) $\exists \, a, b \in \text{M}$ with $e = ab$, $f = ba$

Given $e = ab$, then any $m \in \text{Me}$ has $f = ba$,

$ma = mea = maba = maf \in \text{Mf}$

Giving an $\text{M}$-set map $\text{Me} \xrightarrow{\psi} \text{Mf}$

$m \mapsto ma$

Likewise get an $\text{M}$-set map $\text{Me} \xleftarrow{\phi} \text{Mf}$

$mb \mapsto 1_m$

and can check they're inverses:

$\psi(\phi(m)) = mab = me = m$

$\phi(\psi(m)) = mba = mf = m$
(iii) \exists a, b \in M \text{ with } e = ab, f = ba

\[
\therefore
\]

(v) \quad \text{MeM} = \text{MfM} \quad \text{(i.e. } e \circ f \text{.)}

\[
\therefore
\]

(i) \quad \text{Me} \cong \text{Mf} \quad \text{as (left-) M-sets}

Assuming (iii), one has
\[
\text{MeM} = \text{Me} \circ \text{Me} = \text{MababM} \subseteq \text{MbaM} = \text{MfM}
\]
and \text{MfM} \subseteq \text{MeM} is similar, so (v) follows.

Assuming (v), so \text{MeM} = \text{MfM},
\[
\text{write } f = \text{xy}e, \text{ so } f \circ f = \text{xyef}
\]
and \text{Mf} = \text{Mxyef} \subseteq \text{Myef} \subseteq \text{Mf} \Rightarrow \text{Mf} = \text{Myef}

Hence get a ! M-set map \( \text{Me} \xrightarrow{\varphi} \text{Mf} \)
\[
\text{e} \xrightarrow{\text{eff}} \text{eyf}
\]
which surjects since \text{Mf} = \text{Myef}, showing \(|\text{Me}| \geq |\text{Mf}|\).
Symmetrically \(|\text{Mf}| \geq |\text{Me}|\), so \( \varphi \) is an M-set bijection \( \square \)
Next we learn of a cancellation property called **stability**, that finiteness of $M$ provides:

**THM 1.13**

$\forall m \in M \exists n \in M \ni Mm = M \times m \times M$  

(left-right \hspace{1cm} and \hspace{1cm} right-left \hspace{1cm} dually)  

$M \times m = M \times M \times m$  

$\forall m \in M \exists n \in M \ni Mm = M \times m \times M$  

**proof:** Assume $MmM = M \times m \times M$,  

so $m = u \times m \times v$.  

Then $M \times m \subseteq Mm = M \times m \times M \times m \times v \leq M \times m \times v$  

Subjectivity here  

$\Rightarrow |M \times m| \geq |M \times m \times v|$  

$\Rightarrow$ equality in $(*)$, as desired
Two consequences of stability...

**COR 1.14** \( m_1 \not\leq m_2 \) (i.e. \( Mm_1M = Mm_2M \))

\[ \iff \exists r \in M \text{ with } Mm_1 = Mr, rM = m_2M \]

i.e. \( m_1 \not\leq r, \, r \not\leq m_2 \)

(and left-right dually \( \iff \exists r \in M \text{ with } m_1M = rM, \, Mr = Mm_2 \))

i.e. \( m_1 \not\leq r, \, r \not\leq m_2 \)

### Proof:
Note that \( \iff \) is clear (since \( xLy \Rightarrow xLy \), \( xLy \Rightarrow xLy \)).

For \( \Rightarrow \), assume \( m_1 \not\leq m_2 \)

and write \( m_1 = um_2v \), then set \( r := xM_1 \).

\[ m_2 = xM_1y \]

One has \( xryv = uxM_1yv = um_2v = m_1 \)

so \( MxM_1M = MrM = Mm_1M \)

and Stability gives \( MxM_1 = Mr = Mm_1 \)

Also \( m_2 = ry \) and \( r = xM_1 = xum_2v \),

so \( MrM = Mm_2M = MryM \) and Stability gives \( rM = ryM = m_2M \)
COROLLARY 1.15

The group $G$ of units of $M$ has $G = J_1 = \mathcal{J}_{\text{of } 1}$,

and if $M \setminus G \neq \emptyset$ then it is an ideal.

proof:

$G \leq J_1$: Any unit $g$ has $1 = \bar{g} \cdot g \cdot 1 \in MgM$

(and $g \in G = M \cap M$)

$J_1 \leq G$: if $m \in J_1$ so $MmM = M = M \cap M$

then $Mm = Mm$ and $mM = mM$

$\Rightarrow$ Stability $Mm = M \cap M = mM \Rightarrow m \in G$.

$m \in 1$

To see $M \setminus G$ is an ideal when non-$0$, note

$M \setminus G = M \setminus J_1 = \{meM : 1 \notin MmM\}$

$= I(1)$ from before,

an ideal. ✷