UMN Semigroups seminar Sept. 28, 2021

§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 $\{\underbrace{s^0}_{=1}, s^1, s^2, s^3, \ldots\}$)

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

$$\begin{tikzcd}
s \arrow[r, "\cdot s"] & s^2 \arrow[r, "\cdot s"] & s^3 \arrow[r, "\cdot s"] & s^4 \arrow[r] & s^5 \arrow[r] & s^6 \arrow[r] & s^7 \arrow[dr] & \\
 & & & & & s^{11} \arrow[ur] & & s^8 \arrow[d] \\
 & & & & & s^{10} \arrow[u] & & s^9 \arrow[ll]
\end{tikzcd}$$

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 $\omega \equiv 0 \bmod d$ and $\omega \geq c$.
- Furthermore, e is the identity element for $C := \{s^c, s^{c+1}, s^{c+2}, \ldots\}$ which is a subgroup of S
- $C \cong \mathbb{Z}/d\mathbb{Z}$ is a cyclic group generated by $s^{\omega+1} = s^\omega \cdot s$

EXAMPLE

$$s \to s^2 \to s^3 \to s^4 \to s^5 \to s^6 \to s^7 \to s^8 \to s^9 \to s^{10} \to s^{11} \to s^7$$

$$s^{\omega+1} = s^{11} \qquad e = s^\omega = s^{10}$$

index $c = 7$

period $d = 5$

$\omega = 10 \equiv 0 \bmod 5$
≥ 7

$C \cong \mathbb{Z}/5\mathbb{Z}$

REMARK 1.3

If $n = |S|$ then $\forall s \in S$, more concretely

this idempotent $e = s^{\omega} = s^{n!}$

since both $c, d \leq |S| = n \Rightarrow \begin{cases} n! \geq n \geq c \\ n! \equiv 0 \mod d \end{cases}$

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

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

proof: $\varphi(E(S)) \subseteq E(T)$ since

$$e^2 = e \Rightarrow \varphi(e^2) = \varphi(e)$$
$$\varphi(e^2) = \varphi(e)^2$$

For surjectivity $E(S) \xrightarrow{\varphi} E(T)$, given $e \in E(T)$, note $\varphi^{-1}(e)$ is nonempty (φ surjects) 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.

Idempotents will exist!

1 exists

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 $I_1 I_2 \cdots I_n$ where $I_1, \ldots, I_n$ are all of its ideals)

EXAMPLE

(1) $M = M_n(k) = \{n\times n \text{ matrices over a field } k\}$

has its only ideals $I_r = \{\text{matrices of rank} \le r\}$

unique minimal ideal

$$\underset{\{0_{n\times n}\}}{\underset{\|}{I_0}} \subset I_1 \subset \dots \subset I_{n-1} \subset \underset{M_n(k)}{\underset{\|}{I_n}} \qquad \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right]$$

Right ideals are of form $\{\text{matrices } A \text{ with } \mathrm{im}(A) \subseteq V\}$,

Left ideals are of form $\{\text{matrices } A \text{ with } \ker(A) \supseteq U\}$

for any choices of subspaces $U, V \subset k^n$

EXERCISE: Check me using $\mathrm{im}(AB) \subseteq \mathrm{im}(A)$, $\ker(BA) \supseteq \ker(A)$.

---

(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 $m \notin MsM \Rightarrow m \notin MasbM \subseteq MsM$)

$I(m) = \phi \Leftrightarrow m \in$ minimal ideal

e.g. in $M_n(k)$,
$I(A) = \{B : \mathrm{rank}\, B < \mathrm{rank}\, A\}$

DEF'N: Green's relations (J.A. Green 1951)

Say $m_1 \mathcal{J} m_2$ if $Mm_1M = Mm_2M$ (same principal ideal)

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

$m_1 \mathcal{R} m_2$ if $m_1M = m_2M$ (same principal right ideal)

EXAMPLES

(1) For $M = M_n(k)$ $n \times n$ matrices

$A \mathcal{J} B \iff$ rank A = rank B (so $B = PAQ$ with $P, Q \in GL_n(k)$)

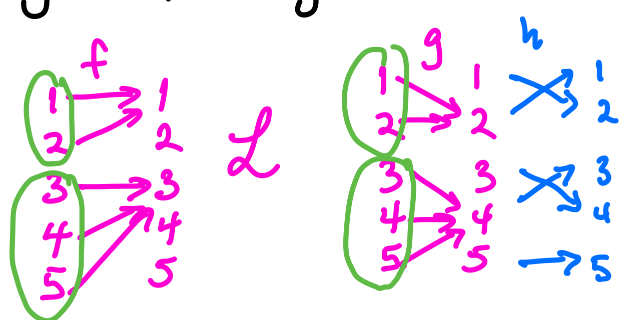
$A \mathcal{L} B \iff A, B$ are row-equivalent (so $B = PA$)

$A \mathcal{R} B \iff A, B$ are column-equivalent (so $B = AQ$)

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

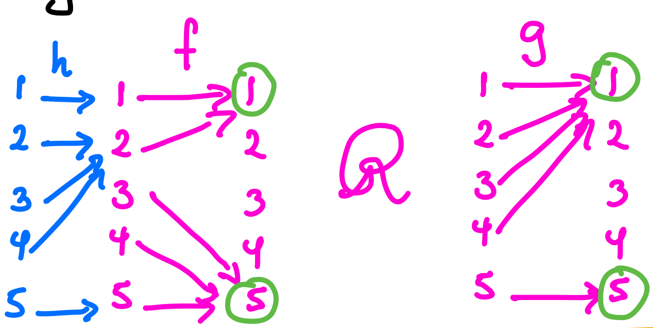
Full transformation monoid of degree n

$f \mathcal{L} g \iff f, g$ have same partition of source into fibers $f^{-1}(i), g^{-1}(i)$



$f \mathcal{L} g$ since $f = h \circ g$, $g = h^{-1} \circ f$

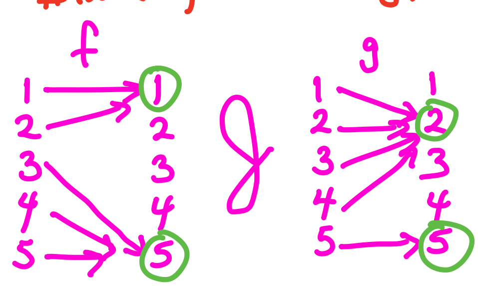
$f \mathcal{R} g \iff \mathrm{im}(f) = \mathrm{im}(g)$



$f \mathcal{R} g$ since $g = f \circ h$

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

$f \mathcal{J} g \iff \#\mathrm{im}(f) = \#\mathrm{im}(g)$



$\Rightarrow T_n$ has ideals

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

$I_1 = \{\text{constant maps}\}$, $I_n = T_n$

where

$$I_r = \{f : \#\mathrm{im}(f) \le r\}$$

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

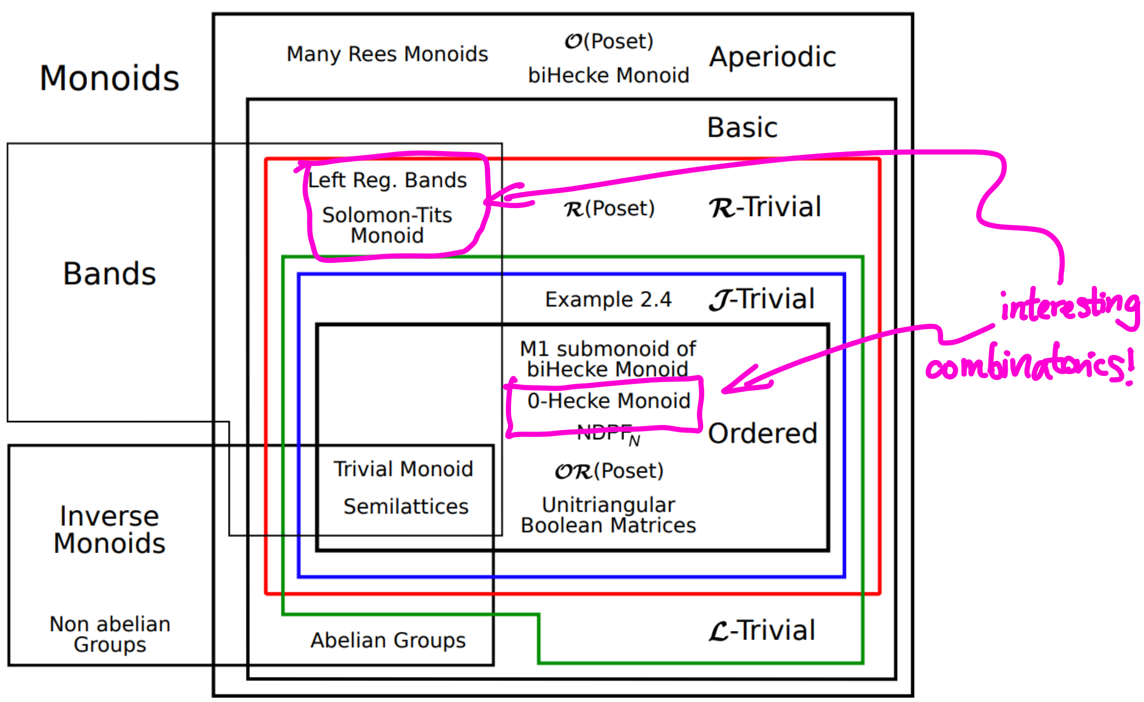
---

NOTE

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

COR 1.14 ahead

From Denton, Hivert, Schilling, Thiery 2011:



Note groups are not $\mathcal{J}, \mathcal{R}, \mathcal{L}$-trivial: $g \mathcal{R} g'$, $g \mathcal{L} g'$ $\forall g, g'$

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

$$m_1 \mathcal{R} m_2 \text{ in } M \iff m_1 \mathcal{R} m_2 \text{ in } eMe$$

and same for $\mathcal{L}, \mathcal{J}$.

proof: Do the proof for $\mathcal{J}$; for $\mathcal{R}, \mathcal{L}$ is similar.

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

$$\iff \exists a,b,c,d \in eMe \text{ with } \begin{array}{l} m_1 = a m_2 b \\ m_2 = c m_1 d \end{array}$$

$$\Rightarrow \quad Mm_1M = Mm_2M.$$

Conversely, if $Mm_1M = Mm_2M$ then

$$eMe \cdot m_1 \cdot eMe \underset{\substack{\uparrow \\ m_1 \in eMe}}{=} eMm_1Me = eMm_2Me \underset{\substack{\uparrow \\ m_2 \in eMe}}{=} eMe \cdot m_2 \cdot eMe \quad \blacksquare$$

M-sets

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

a map $M \times X \longrightarrow X$
$(m, x) \longmapsto mx$

with $1 \cdot x = x \quad \forall x \in X$
$m_1(m_2 x) = (m_1 m_2) x$

Call it a faithful action if $mx = m'x \ \forall x \in X \implies m = m'$ in M

A $\overset{\text{set-}}{\text{map}}$ $X \xrightarrow{\varphi} Y$ is M-equivariant if
$$\varphi(mx) = m\varphi(x) \quad \forall \begin{smallmatrix} m \in M \\ x \in X \end{smallmatrix}$$

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

$$\mathrm{Hom}_M(X, Y) = \{M\text{-equivariant } X \xrightarrow{\varphi} Y\}$$

PROP 1.8: For an M-set X and $e \in E(M)$
$\overset{\shortparallel}{e^2}$

(i) one has a bijection $\mathrm{Hom}_M(Me, X) \xrightarrow{\sim} eX$
$\varphi \longmapsto \varphi(e)$.

Take $X = Me$

(ii) $\mathrm{End}_M(Me) \cong (eMe)^{op}$ as monoids

apply $\underset{\text{monoid}}{A} \longmapsto \underset{\text{group of units}}{A^\times}$

(iii) $\mathrm{Aut}_M(Me) \cong (G_e)^{op}$ as groups
where $G_e :=$ group of units in eMe.

PROP 1.8: For an M-set X and $\underset{\overset{\shortparallel}{e^2}}{e} \in E(M)$

(i) one has a bijection $\begin{array}{ccc} \mathrm{Hom}_M(Me, X) & \xrightarrow{\sim} & eX \\ \varphi & \longmapsto & \varphi(e). \end{array}$

(ii) $\mathrm{End}_M(Me) \cong (eMe)^{op}$ as monoids

(iii) $\mathrm{Aut}_M(Me) \cong (G_e)^{op}$ as groups

where $G_e :=$ group of units in eMe.

---

proof: If $\varphi \in \mathrm{Hom}_M(Me, X)$, then $\varphi(e) \in eX$

since $\varphi(e) = \varphi(e^2) = e\varphi(e)$, and $\varphi(e)$ determines φ

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

is $\begin{array}{ccc} \mathrm{Hom}_M(Me, X) & \longleftarrow & eX. \\ (\varphi : me \mapsto \underset{\overset{\shortparallel}{mex}}{mx}) & \longleftarrow\!\shortmid & \underset{\overset{\shortparallel}{ex}}{x} \end{array}$

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 $\underset{\text{monoid}}{A} \longmapsto \underset{\text{group of units}}{A^\times}$ $\blacksquare$

REMARK 1.9: If one doesn't like the "op"'s,

(ii) $\mathrm{End}_M(Me) \cong (eMe)^{op}$

says eMe acts on the right of Me via M-set maps, and gives all such maps.

Likewise, (iii) $\mathrm{Aut}_M(Me) \cong (G_e)^{op}$

says G_e acts (as a group) on the right of Me.

PROP 1.10:

G_e (right-)acts freely on L_e = $\mathcal{L}$-class of e
= generators of Me

(and (left-)acts freely on R_e = $\mathcal{R}$-class of e).

proof: For action, if $m \in L_e$ and $g \in G_e = (eMe)^\times$,

want $mg \in L_e$, that is $Me \overset{?}{=} Mmg$:

"$\supseteq$": $g = ege \Rightarrow Mmg = Mmege \subseteq Me$

"$\subseteq$": $m \in L_e \Rightarrow \exists\, y \in M$ with $e = ym$

so $e = g^{-1}g = g^{-1}eg = g^{-1}ymg$

and $Me = Mg^{-1}ymg \subseteq Mmg$

For freeness, using same m, g, y as above if $mg = m$ then $g = eg = ymg = ym = e$. $\blacksquare$

EXAMPLE When $M = M_n(k)$ = $n \times n$ matrices, a typical idempotent $e \in \mathcal{E}(M)$ is

$$e = \begin{array}{cc} & \begin{array}{cc} V_1 & V_2 \end{array} \\ \begin{array}{c} V_1 \\ V_2 \end{array} & \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] \end{array} \quad \text{where } V = k^n = \underbrace{V_1}_{\dim r} \oplus \underbrace{V_2}_{\dim n-r}$$

having $eMe = \left\{ \left[\begin{array}{c|c} A & 0 \\ \hline 0 & 0 \end{array}\right] : A \in M_r(k) \right\}$

$$G_e = (eMe)^\times = \left\{ \left[\begin{array}{c|c} A & 0 \\ \hline 0 & 0 \end{array}\right] : A \in GL_r(k) \right\}$$

and the generators L_e of $Me = \left\{ \left[\begin{array}{c|c} A & 0 \\ B & 0 \end{array}\right] \right\}$ have lin. indep. 1st r columns, carrying a free action of G_e on the right.

$$\left[\begin{array}{c} G_e\text{-orbits} \\ \text{on } L_e \end{array} \longleftrightarrow \begin{array}{c} r\text{-dim'l subspaces of } k^n \\ \text{given by colspace of } \left[\begin{array}{c|c} A & 0 \\ \hline B & 0 \end{array}\right] \end{array} \right]$$

Now can relate M-set structure for Me, eM to Green's $\mathcal{J}$.

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

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

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

(iii) $\exists\, a, b \in M$ with $\begin{array}{l} e = ab \\ f = ba \end{array}$

clear $\Uparrow$

(iv) $\exists\, x, x' \in M$ with $\begin{array}{l} xx'x = x \\ x'xx' = x' \end{array}$ and $\begin{array}{l} e = x'x \\ f = xx' \end{array}$

(v) $MeM = MfM$ (i.e. $e \mathcal{J} f$.)

Note an immediate --

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

(since $eMe \cong \mathrm{End}_M(eM)$ and $G_e = (eMe)^\times$).

EXAMPLE: Recall for $M = M_n(k)$

$$e \mathcal{J} f \iff \mathrm{rank}(e) = \mathrm{rank}(f)$$

So if we have idempotents $e, f \in E(M)$ with $e \mathcal{J} f$ then one can write

$$\begin{tikzcd}
V = k^n = \mathrm{im}(e) \arrow[d, shift left, "b"] & \oplus & \underbrace{\ker(e)} \arrow[dr, "b"] & \\
 & & & \{0\} \\
= \mathrm{im}(f) \arrow[u, shift left, "a"] & \oplus & \underbrace{\ker(f)} \arrow[ur, "a"'] &
\end{tikzcd}$$

pick some inverse isomorphisms

Then $\quad e = ab = \begin{array}{cc} & \begin{array}{cc} \mathrm{im}\,e & \ker e \end{array} \\ \begin{array}{c} \mathrm{im}\,e \\ \ker e \end{array} & \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & 0 \end{array}\right] \end{array}$

$$f = ba = \begin{array}{cc} & \begin{array}{cc} \mathrm{im}\,f & \ker f \end{array} \\ \begin{array}{c} \mathrm{im}\,f \\ \ker f \end{array} & \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & 0 \end{array}\right] \end{array}$$

proof of ...

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

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

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

(iii) $\exists\, a, b \in M$ with $\begin{array}{l} e = ab \\ f = ba \end{array}$

clear $\Uparrow$

(iv) $\exists\, x, x' \in M$ with $\begin{array}{l} xx'x = x \\ x'xx' = x' \end{array}$ and $\begin{array}{l} e = x'x \\ f = xx' \end{array}$

(v) $MeM = MfM$ (i.e. $e \mathcal{J} f$.)

Proof Strategy:

Show
$$\begin{tikzcd}
 & (i) \arrow[r, Rightarrow] & (iv) \arrow[dl, Rightarrow] \\
(v) \arrow[ur, Rightarrow] & (iii) \arrow[l, Rightarrow] \arrow[u, Rightarrow] &
\end{tikzcd}$$

(and replacing (i) by (ii) follows by left-right symmetry)

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

$\Downarrow$

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

Given inverse M-set isomorphisms $Me \underset{\psi = \varphi^{-1}}{\overset{\varphi}{\rightleftarrows}} Mf$,

let $x' := \varphi(e)$ $\quad\left[= \varphi(ee) = e\varphi(e) \in eMf\right.$

$x := \psi(f)$ $\quad\left.= \psi(ff) = f\psi(f) \in fMe\right]$

and check

$$x'x = x'\psi(f) = \psi(x'f) = \psi(x') = \psi(\varphi(e)) = e$$

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

Also $x'xx' = ex' = x'$ since $x' \in eMf$

and $xx'x = fx = x$ since $x \in fMe$

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

$\Uparrow$

(ii) $\exists a, b \in M$ with $\begin{array}{l} e = ab \\ f = ba \end{array}$

Given $\begin{array}{l} e = ab \\ f = ba \end{array}$, then any $m \in Me$ has

$$\underset{\substack{\uparrow \\ m \in Me}}{ma = mea} \underset{\substack{\uparrow \\ e=ab}}{=} maba \underset{\substack{\uparrow \\ f=ba}}{=} maf \in Mf$$

giving an M-set map $\begin{array}{ccc} Me & \xrightarrow{\varphi} & Mf \\ m & \longmapsto & ma \end{array}$

Likewise get an M-set map $\begin{array}{ccc} Me & \xleftarrow{\psi} & Mf \\ mb & \longleftarrow\!\shortmid & m \end{array}$,

and can check they're inverses:

$$\psi(\varphi(m)) = mab = me = m$$
$$\varphi(\psi(m)) = mba = mf = m$$

(iii) $\exists a, b \in M$ with $\begin{matrix} e = ab \\ f = ba \end{matrix}$

$\Downarrow$

(v) $MeM = MfM$ (i.e. $e \mathcal{J} f$.)

$\Downarrow$

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

Assuming (iii), one has

$$MeM = MeeM = MababM \subseteq MbaM = MfM$$

and $MfM \subseteq MeM$ is similar, so (v) follows.

Assuming (v), so $MeM = MfM$,

write $f = xey$, so $f = ff = xeyf$

and $Mf = Mxeyf \subseteq Meyf \subseteq Mf \Rightarrow Mf = Meyf$

Hence get a ! M-set map $\begin{matrix} Me \xrightarrow{\varphi} Mf \\ e \longmapsto eyf \end{matrix}$

which surjects since $Mf = Meyf$, showing $|Me| \geq |Mf|$.

Symmetrically $|Mf| \geq |Me|$, so φ is an M-set bijection $\blacksquare$

Next we learn of a cancellation property called stability, that finiteness of M provides:

THM 1.13

$$MmM = MxmM \quad \left(\begin{array}{c}\text{and} \\ \text{left-right} \\ \text{dually}\end{array} \quad \begin{array}{c} MmM = MmxM \\ \Updownarrow \\ mM = mxM \end{array}\right)$$

$\Uparrow$ clear

$\Downarrow$ not clear

$$Mm = Mxm$$

---

proof: Assume $MmM = MxmM$,

so $m = uxmv$.

Then $Mxm \overset{(*)}{\subseteq} Mm = Muxmv \subseteq Mxmv$ $\quad zv$

$\uparrow$ $\quad$ $\uparrow$

Mxm $\quad z$

surjectivity here

$\Rightarrow |Mxm| \geq |Mxmv|$

$\Rightarrow$ equality in $(*)$, as desired ∎

Two consequences of stability ...

COR 1.14 $m_1 \mathcal{J} m_2$ (i.e. $Mm_1M = Mm_2M$)

$\iff$ $\exists\, r \in M$ with $Mm_1 = Mr$, $rM = m_2M$

i.e. $m_1 \mathcal{L} r$, $r \mathcal{R} m_2$

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

i.e. $m_1 \mathcal{R} r$, $r \mathcal{L} m_2$

---

proof: Note that $\Leftarrow$ is clear (since $x \mathcal{L} y \Rightarrow x \mathcal{J} y$, $x \mathcal{R} y \Rightarrow x \mathcal{J} y$).

For $\Rightarrow$, assume $m_1 \mathcal{J} m_2$

and write $m_1 = u m_2 v$, $m_2 = x m_1 y$, then set $r := x m_1$.

One has $u r y v = u x m_1 y v = u m_2 v = m_1$

so $M x m_1 M = M r M = M m_1 M$

and Stability gives $M x m_1 = M r = M m_1$

Also $m_2 = r y$ and $r = x m_1 = x u m_2 v$,

so $MrM = Mm_2M = MryM$ and Stability gives

$rM = ryM = m_2M$ ∎

COROLLARY 1.15

The group G of units of M has $G = J_1 = \mathcal{J}$-class of 1, and if $M \setminus G \neq \emptyset$ then it is an ideal.

proof:

$G \subseteq J_1$: Any unit g has $1 = g^{-1} \cdot g \cdot 1 \in MgM$ (and $g \in M = M1M$)

$J_1 \subseteq G$: if $m \in J_1$ so $MmM = M = M1M$

then $M1m = Mm$ and $m1M = mM$

$$\xRightarrow{\text{Stability}} \quad Mm = \underset{\substack{\| \\ M \ni 1}}{M1M} = mM \Rightarrow m \in G.$$

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

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

$= I(1)$ from before, an ideal. ∎