Monoidi e Semigruppi

e.paracucchi
m.romeo

April 2021

1 Introduzione

Definizione 1.1. Un insieme M dotato di una operazione $* : M \times M \longrightarrow M$ si dice *Semigruppo* se $*$ è associativa. Si dice $Monoide$ se è un semigruppo ed ammette un elemento neutro: $\exists e_M \in M$ tale che $\forall m \in$ si abbia $a * e_M = e_M * a = a$.

Osservazione 1.1. M monoide è anche un semigruppo.

Esempio 1. Esempi di monoidi sono $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$. Esempi di semigruppi sono $(\mathbb{N} \setminus \{0\}, +)$, $(\mathbb{Z} \setminus \{1\}, \cdot)$.

Definizione 1.2. Sia S un semigruppo con l'operazione $*$ e sia $N \subset S$. Allora N si dice *sotto-semigruppo* se è chiuso per $*$, si denota con $N < S$. Sia M un monoide con l'operazione $*$ e sia $N \subset M$. Allora N si dice *sotto-monoide* se è chiuso per $*$ e $e_M \in N$, si denota con $N < M$. inoltre se N ha struttura di gruppo si dice che è $sotto-gruppo$ di M, e si denota allo stesso modo.

Definizione 1.3. Sia M un monoide, $G(M) = \{a \in M | \ \exists b \in M, \ a * b = e_M\}$.

Osservazione 1.2. Sia M un monoide, allora $G(M)$ è un sotto-gruppo di M.

Proposizione 1.1. *Sia M un monoide, allora $M \setminus G(M)$ è un sotto-semigruppo di M.*

Dimostrazione. Siano $a, b \in M \setminus G(M)$. Se per assurdo $ab \in G(M)$ allora esiste $c \in G(M)$ tale che $abc = e_M$, ma allora a è invertibile, assurdo. □

Proposizione 1.2. *Sia S un semigruppo finito. Allora esiste $c \in S$ idempotente.*

Dimostrazione. Sia $a \in S$. Se a é idempotente abbiamo fatto, se no sia $b = a^2$. Se b é idempotente abbiamo fatto, se no iteriamo questa procedura ottenendo così la successione

$$\begin{cases} a_1 = a \\ a_n = (a_{n-1})^2 \quad n > 1 \end{cases}$$

dunque o otteniamo un idempotente oppure, per finitezza di S, esistono $k, n_0 \in \mathbb{N}$, con $k \leq n_0$, tale che $(a_{n_0})^2 = a_k$. Considero allora $c = a_k a_{k+1} \dots a_{n_0-1} a_{n_0}$. Osserviamo che ogni a_i, con $i \leq n_0$, è potenza di a_1, dunque commutano tutti fra di loro, e di conseguenza:

$$c^2 = (a_k a_{k+1} \dots a_{n_0-1} a_{n_0})^2 = a_k a_{k+1} \dots a_{n_0-1} a_{n_0} \cdot a_k a_{k+1} \dots a_{n_0-1} a_{n_0} =$$
$$= a_k a_{k+1} \dots a_{n_0-1} (a_{n_0} a_{n_0}) \cdot a_k a_{k+1} \dots a_{n_0-1} = a_k a_{k+1} \dots a_{n_0-1} \ a_{n_k} a_k a_{k+1} \dots a_{n_0-1} = \dots$$
$$\dots = a_k a_{k+1} \dots a_{n_0-1} (a_{n_0-1} a_{n_0-1}) = c.$$
□

Osservazione 1.3. Se M é un monoide finito allora ammette un idempotente non banale, infatti $M \setminus G(M)$ è un sotto-semigruppo di M e per la proposizione precedente ammette c idempotente.

Definizione 1.4. Siano T, S semigruppi. Allora $f : T \longrightarrow S$ si dice $omomorfismo$ tra semigruppi, o più semplicemente $omomorfismo$, se $\forall\ a, b \in T$ si ha che $f(ab) = f(a)f(b)$. Siano M, N mnoidi. Allora $f : M \longrightarrow N$ si dice $omomorfismo$ tra monoidi, o più semplicemente $omomorfismo$, se è un omomorfismo tra semigruppi e $f(e_M) = e_N$.

Definizione 1.5. Sia M un semigruppo o un monoide, diciamo che M è *estendibile* ad un gruppo se esiste un gruppo G ed una mappa $f : M \longrightarrow G$ tale che f è un omomorfismo iniettivo.

Teorema 1.1. *Sia S un semigruppo finito. Allora o S è un gruppo oppure non è estendibile.*

Dimostrazione. Supponiamo che S non sia un gruppo, allora per la proposizione 1.2 ammette un idempotente b. Considero il caso in cui S non sia un monoide. Per ogni gruppo G e per ogni omomorfismo $f : S \longrightarrow G$ osserviamo che $f(b)^2 = f(b^2) = f(b)$, dunque $f(b)$ è idempotente in G, inoltre in G esiste un elemento c tale che $f(b)c = e_G$, cioè l'inverso di $f(b)$, e dunque $e_G = f(b)c = f(b)^2c = f(b)f(b)c = f(b)$. Ma allora, siccome S non ha un elemento neutro, esisterà un d tale che $d \neq db$, ma $f(db) = f(d)f(b) = f(d)e_G = f(d)$, quindi f non è iniettiva. $\square$

Corollario 1.1. *Sia M un monoide finito. Allora o M è un gruppo oppure non è estendibile.*

Dimostrazione. Supponiamo che M non sia un gruppo, e supponiamo per assurdo che M sia estendibile, dunque esiste un gruppo G ed un omomorfismo iniettivo $f : M \longrightarrow G$. Ma $M \setminus G(M)$ è un semigruppo finito ma non un gruppo, dunque non è estendibile per il teorema precedente, però l'inclusione $i : M \setminus G(M) \longrightarrow M$ è un omomorfismo iniettivo e quindi $i \circ f$ è un omomorfismo iniettivo da $M \setminus G(M)$ in G che è assurdo. $\square$

Definizione 1.6. a) Sia M un semigruppo o un monoide, allora $I(M) = \{a \in M |\ a^2 = a\}$ è l'inisme degli idempotenti;
b) Siano M, N con M semigruppo o monoide, e N monoide; e sia $f : M \longrightarrow N$ un omomorfismo. Allora $Ker(f) = \{a \in M |\ f(a) = e_N\}$ e $Imm(f) = \{b \in N |\ \exists\ a \in M,\ f(a) = b\}$.

Osservazione 1.4. $Ker(f)$ e $Imm(f)$ sono sotto-semigruppi rispettivamente di M e N, inoltre se M è monoide allora sono anche sotto-monoidi. Se M è un semigruppo commutativo allora $I(M)$ è un sotto-semigruppo commutativo e se M è un monoide commutativo allora $I(M)$ è un sotto-monoide commutativo.

Definizione 1.7. Sia M un semigruppo e X un insieme. La mappa $\cdot : M \times X \longrightarrow X$ si dice *azione* di M su X ($M \curvearrowright X$) se :
a) $\forall\ a, b \in M,\ \forall x \in X$ si ha che $a \cdot (b \cdot x) = (a *_M b) \cdot x$;
(b) $\forall\ x \in X$ si ha che $e_M \cdot x = x$ (nol caso M sia un monoide).

Osservazione 1.5. $G(M) \curvearrowright M$; $G(M) \curvearrowright M \setminus G(M)$; $M \curvearrowright M$; $M \curvearrowright M \setminus G(M)$, tutte col semplice prodotto. $G(M)$ agisce inoltre con l'azione di coniugio.

Definizione 1.8. Supponiamo che M agisca su N, allora chiamiamo *orbita* dell'elemento $x \in N$ l'insieme $orb(x) = \{m \cdot x |\ m \in M\}$ e chiamiamo *stabilizzatore* dell'elemento $x \in N$ l'insieme $stab(x) = \{m \in M |\ m \cdot x = x\}$.

Osservazione 1.6. Lo stabilizzatore è un sotto-monoide di M, infatti se $n, m \in stab(x)$, allora $(nm) \cdot x = n \cdot (m \cdot x) = n \cdot x = x$.

Definizione 1.9. Sia M un monoide o un semigruppo e $N \subset M$. Allora N si dice *normale* se per ogni $a \in M$ si ha che $aN \subset N$, si dice anche *ideale*.

Definizione 1.10. Sia M un monoide e $S \subset M$ un sotto-insieme. Chiamiamo *normalizzatore* dell'insieme S l'insieme $N(S)$ che è il più piccolo sotto-semigruppo normale di M che contiene S. Chiamiamo $H(S)$ il più piccolo sotto-semigruppo di M che contiene S.

Osservazione 1.7. L'osservazione precedente è buona infatti considero $\Gamma = \{H\ sotto-semigruppi\ normali\ di\ M|\ S \subset H\}$, che è non vuoto in quanto ci sta M stesso, con l'ordinamento parziale $\succ$ tale che $H \succ K$ se e solo se $H \subset K$. Se ho una catena $\{H_i\}$ allora $\bigcap\limits_i H_i$ è elemento maggiorante della catena, e quindi per zorn esiste massimale H, ed è unico infatti se H, K sono due massimali allora $H \cap K$ è un sotto-semigruppo che contiene S ed è normale in quanto per normalità di H si ha $a(H \cap K) \subset aH \subset H$ e per normalità di K si ha $a(H \cap K) \subset aK \subset K$. In maniera analoga si mostra la buona definizione di $H(S)$.

Osservazione 1.8. L'estendibilità di un monoide o di un semigruppo ci può aiutare a capire se esistono o meno omomorfismi iniettivi tra di essi, infatti : vogliamo capire se esiste un omomorfismo iniettivo $i : M \longrightarrow N$; se N fosse estendibile ed M no allora siamo certi che se i è un omomorfismo, allora non può essere iniettivo in quanto se per assurdo lo fosse allora esisterebbe un gruppo G ed un omomorfismo iniettivo $f : N \longrightarrow G$, ma allora $f \circ i$ è un omomorfismo iniettivo tra M e G, che è assurdo.

Definizione 1.11. Sia M un semigruppo o un monoide estendibile, e sia G gruppo in cui si immerge tramite $f : M \longrightarrow G$. Definisco $M^{-1}(G) = \{b \in G|\ \exists a \in M\ t.c\ f(a)b = e_G\}$.

Osservazione 1.9. Osserviamo che $M^{-1}(G)$ è un sotto-monoide di G ed è isomorfo ad M, cioè esiste biunivoco un omomorfismo tra $M^{-1}(G)$ e M, infatti la mappa $j : M \longrightarrow M^{-1}(G)$ tale che $j(a) = f(a)^{-1}$ è isomorfismo, dove $f : M \longrightarrow G$ è omomorfismo iniettivo.

Definizione 1.12. Sia M Un monoide o un semigruppo, e siano $M_1, \ldots, M_n$ sottoinsiemi di M. Allora $M_1 \otimes \cdots \otimes M_n = \{ \prod\limits_{finiti} a_1 *_M \cdots *_M a_n|\ a_i \in M_i\}$ è il $sotto-semigruppo$ o $sotto-monoide$ generato dagli M_i.

Osservazione 1.10. Osserviamo che se gli M_i sono monoidi, allora $M_1 \otimes \cdots \otimes M_n = H(\bigcup\limits_{i=1,\ldots,n} M_i)$, infatti vale $M_1 \otimes \cdots \otimes M_n \subset H(\bigcup\limits_{i=1,\ldots,n} M_i)$, $\bigcup\limits_{i=1,\ldots,n} M_i \subset M_1 \oplus \cdots \oplus M_n$ e per minimialità di $H(\bigcup\limits_{i=1,\ldots,n} M_i)$ si ha l'uguaglianza. Nel caso di semigruppi non è detto che valga $\bigcup\limits_{i=1,\ldots,n} M_i \subset M_1 \otimes \cdots \otimes M_n$.

Definizione 1.13. Siano M, N monoidi o semigruppi. Allora $M \times N = \{(a, b)|\ a \in M\ b \in N\}$.

Osservazione 1.11. $M \times N$ è un semigruppo con l'perazione $(a, b) * (c, d) = (a *_M c, b *_N d)$, se M, N sono entrambi monoidi allora anche $M \times N$ lo è, dove l'elemento neutro è (e_M, e_N).

Osservazione 1.12. Sia M monoide, allora $M \setminus G(M)$ è un sotto-semigruppo normale.

Definizione 1.14. Sia M un monoide o un semigruppo e siano H, K sotto monoidi o sotto semigruppi, allora definisco $H \rtimes_\phi K$ come l'insieme $H \times K$ dotato dell'operazione $(a, b) * (c, d) = (a *_H \phi(b)(c), b *_K d)$ dove $\phi : K \longrightarrow End(H)$ è un omomorfismo.

Osservazione 1.13. $H \rtimes_\phi K$ della definizione precendente è un semigruppo, e se H, K sono entrambi monoidi allora anche $H \rtimes_\phi K$ lo è, e l'elemento neutro è (e_H, e_K), infatti: $(a, b) * (e_H, e_K) = (a *_H \phi(b)(e_H), b *_K e_K) = (a *_H e_H, b *_K e_K) = (a, b)$ dove ho usato il fatto che per ogni $b \in K$ si ha che $\phi(b)$ è un omomorfismo, inoltre $(e_H, e_K) * (a, b) = (e_H *_H \phi(e_K)(a), e_K *_K b) = (Id_H(a), b) = (a, b)$, dove ho usato che ϕ è un omomorfismo.

Esempio 2. Sia M un monoide o un semigruppo e siano H, K sotto monoidi o sotto semigruppi con H normale e sia $\phi : K \longrightarrow End(H)$ tale che $\phi(a) = a\cdot$, moltiplicazione per a, che è ben definita in quanto H normale. Allora è ben definito $H \rtimes_\phi K$, ma non è detto che si immerga in M. Infatti consideriamo $M = \mathbb{Z}/_{6\mathbb{Z}}$, $H = \{0, 2, 4\}$ e $K = \{0, 3\}$ e sia $A = H \rtimes_\phi K$, ϕ definita come prima. Osserviamo che A ha 6 elementi come M, quindi una immersione in M è anche un isomorfismo, dunque A dovrebbe avere un elemento neutro, ma non esiste nessun elemento in A che moltiplicato per $(2, 0)$ dia come prodotto $(2, 0)$, infatti perso un qualsiasi elemento (a, b) in A si ha $(2, 0) * (a, b) = (2\phi(0)(a), 0b) = (0, 0) \neq (2, 0)$. Se avessimo invece considerato $K = \{0, 1, 3\}$, allora $H \rtimes_\phi K$ sarebbe stato anche di cardinalità maggiore di M.

Osservazione 1.14. sia $f : M \longrightarrow N$ un omomorfismo tra monoidi o semigruppi, allora $f(I(M)) \subset I(N)$, infatti posto $a \in I(M)$ si ha che $f(a)^2 = f(a^2) = f(a)$.

Definizione 1.15. Siano M, N monoidi o semigruppi, allora $Hom(M, N) = \{f : M \longrightarrow N|\ t.c\ f\ omomorfismo\}$; $Hom(M, M) = End(M)$.

Osservazione 1.15. $Hom(M, N)$ é un monoide con la composizione.

Osservazione 1.16. Gli oggetti $Hom(A, \cdot)$ e $Hom(\cdot, A)$ sono funtori.

Proposizione 1.3. *Se ho $i : M \longrightarrow N$ iniettiva, allora $\bar{i} : Hom(A, M) \longrightarrow Hom(A, N)$ é iniettiva, dove $\bar{(i)}(f) = i \circ f$.*

Dimostrazione. Siano $f, g : A \longrightarrow M$ tale che esiste $a \in A$ con $f(a) \neq g(a)$, allora per iniettività $i \circ f(a) \neq i \circ g(a)$, quindi $\bar{i}(f) \neq \bar{i}(g)$. □

Esempio 3. Esempi di monoidi sono $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{K}[x], \cdot)$, $(Mat(n, \mathbb{K}), *)$, $(\mathbb{K}[[x]], \cdot)$ con $*$ il prodotto riga per colonna. Dato M monoide un esempio di sotto-monoide è $\{p^n\}$ dove $p \in M$. Data $f : M \longrightarrow N$ omomorfismo, allora $f(M)$ é sotto-monide di N e per ogni $A < N$ si ha che $f^{-1}(A)$ é sotto-monoide di M.

Proposizione 1.4. *Sia M un semigruppo o un monoide. Allora M ha elementi idempotenti non banali se e solo se ammette almeno un sotto- semigruppi finito.*

Dimostrazione. Se $N < M$ è finito, per la proposizione 1.2, esiste un elemento idempotente non banale. Se invece ho un elemento idempotente non banale c, allora $< c >$ è sotto-semigruppo finito, dove $< c >= \{c^n |\ n \in \mathbb{N}\}$ è il sotto-semigruppo generato da c. □

Definizione 1.16. Sia M un monoide. $dim(M)$ é la "massima lunghezza" di catene di sotto-semigruppi normali di M, cioè $\{e_M\} \subsetneq N_1 \subsetneq \cdots \subsetneq M$. Diciamo che M è *artiniano* se $dim(M) < +\infty$ (vedere def analoga con sotto-semigruppi o sotto-monoidi).

Definizione 1.17. M è un monoide *destro* se è un semigruppo ed esiste $e \in M$ tale che per ogni $a \in M$ si ha che $a * e = a$; analogo per monoide *sinistro* con $e * a = a$. (vedere se lasciarla)

Osservazione 1.17. Sia $A = (\mathbb{N}\backslash\{0\}, +)\times(\mathbb{Z}/_{6\mathbb{Z}}, \cdot)$ e sia $B =< (1,2) >$. Se B si potesse scrivere come prodotto di due sotto-semigruppi M, N rispettivamente di $(\mathbb{N} \setminus \{0\}, +), (\mathbb{Z}/_{6\mathbb{Z}}, \cdot)$, quindi $M \times N$, allora si avrebbe $1 \in M$, $4 \in N$ ma $(1,4) \notin B$, dunque "sotto-semigruppi di un prodotto diretto non sono prodotto diretto di sotto-seemigruppi".

Definizione 1.18. Sia M un monoide. $a \in M$ si dice *distruttore* se per ogni $b \in M$ vale $ab = a$; lo si chiama anche *zero* di M.

Osservazione 1.18. Un elemento distruttore è anche idempotente.

Osservazione 1.19. Sia $f : M \longrightarrow A$ omomorfismo surgettivo. Allora, se a è un distruttore e N un sotto-semigruppo normale di M, allora $f(a)$ è distruttore e $f(N)$ è normale, infatti: Per ogni $b \in A$ esiste $c \in M$ tale che $b = f(c)$ e quindi $bf(a) = f(c)f(a) = f(ca) = f(a)$ e $bf(N) = f(c)f(N) = f(cN) \subset f(N)$.

Osservazione 1.20. Sia M un monoide commutativo, allora l'elemento neutro e il distruttore sono unici, infatti; se e_1, e_2 sono elementi neutri di M allora $e_1 = e_1e_2 = e_2$, e se a, b sono zeri di M allora $a = ab = b$.

Osservazione 1.21. Sia N sottoinsieme normale di M monoide commutativo, e a lo zero di M, allora $a \in N$.

Definizione 1.19. Sia M un monide e a lo zero di M, allora $D(M) = \{b \in M | \, \exists c \in M \ t.c. \ a = bc\}$ é l'insieme dei divisori di a.

Osservazione 1.22. Se M è commutativo allora $D(M)$ è un semigruppo, infatti : posto a distruttore di M e $b, c \in D(M)$, allora esiste $d \in M$ tale che $cd = a$ quindi $bcd = ba = a$, dunque $bc \in D(M)$.

Osservazione 1.23. Se M, N sono estendibili, allora $M \times N$ è estendibile.

Definizione 1.20. Sia M un semigruppo e sia $x \in M$. chiamiamo *ordine* di x il numero $\{x^n | n \in \mathbb{N}\}$.

Osservazione 1.24. Dalla dimostrazione della proposizione 1.2 si evince che ogni elemento x non invertibile di un monoide finito o è idempotente o esiste una potenza n tale che x^n è idempotente.

Definizione 1.21. Sia λ un ordinale. Considero $S_\lambda = \{f : \lambda \longrightarrow \lambda | \ f \text{ è } \textit{biunivoca}\}$.

Osservazione 1.25. S_λ con l'operazione di composizione é un gruppo.

Proposizione 1.5. *Per ogni G gruppo esiste un ordinale λ ed una mappa $f : G \longrightarrow S_\lambda$ tale che f è un omomorfismo iniettivo.*

Dimostrazione. Consideriamo $\succ$ ordinamento che rende $\alpha = (G, \succ)$ ordinale, e consideriamo $\psi : G \longrightarrow S_\alpha$ tale che $\psi(g) : \alpha \longrightarrow \alpha$ con $\psi(g)(s) = gs$. ψ è ben definita infatti se $s \neq t$ allora $gs \neq gt$ e per ogni $s \in \alpha$ si ha $gg^{-1}s$. Inoltre ψ è omomorfismo iniettivo, infatti se $s \neq t$ allora $\psi(s)(e_G) \neq \psi(t)(e_G)$, quindi $\psi(s) \neq \psi(t)$, e $\psi(st)(g) = stg = \psi(s)(tg) = \psi(s)(\psi(t)(g)) = \psi(s) \circ \psi(t)(g)$. (vedere se lasciare il discorso sugli ordinali) $\square$

Osservazione 1.26. Se $\lambda \leq \mu$, ordinali, allora S_λ si immerge come gruppo in S_μ, infatti : $\{f \in S_\mu | \ f|_{\mu\setminus\lambda} = Id_{\mu\setminus\lambda}\}$ é una copia isomorfa di S_λ (da vedere meglio).

Definizione 1.22. $Fun(M, N) = \{f : M \longrightarrow N\}$.

Osservazione 1.27. Se N è un semigruppo, allora $* : Fun(M, N) \times Fun(M, N) \longrightarrow Fun(M, N)$ tale che $f * g(a) = f(a) *_N g(a)$ è una operazione che rende $Fun(M, N)$ un semigruppo. Se N è un monoide allora $Fun(M, N)$ è un monoide infatti f tale che $\forall a \in M$ vale $f(a) = e_N$ è elemento neutro. Infine se N è un gruppo, allora $Fun(M, N)$ è un gruppo, infatti posto f, g tale che $g(a) = f(a)^{-1}$ è l'inversa di f.

Osservazione 1.28. Se N è un monoide commutativo e M un semigruppo, allora $(Hom(M, N), *)$ è un monoide commutativo, infatti $f * g(ab) = f(ab) *_N g(ab) = f(a) *_N f(b) *_N g(a) *_N g(b) = f(a) *_N g(a) *_N f(b) *_N g(b) = f * g(a) *_N f * g(b)$, quindi $f * g$ è un omomorfismo e $f * g(a) = f(a) *_N g(a) = g(a) *_N f(a) = g * f(a)$ cioè $*$ è commutativo.

Osservazione 1.29. Sia M un gruppo commutativo, allora $(End(M), \circ)$ è un monoide e $(End(M), *)$ è un gruppo commutativo, inoltre per ogni $f, g, t \in End(M)$ e per ogni $a \in M$ si ha: $(f * g) \circ t(a) = f \circ t(a) *_M g \circ t(a) = (f \circ t) * (g \circ t)(a)$, e $t \circ f * g(a) = t(f(a) *_M g(a)) = t(f(a) *_M t(g(a) = (t \circ f) * (t \circ g)(a)$. Dunque $(End(M), *, \circ)$ è un anello commutativo.

Proposizione 1.6. *Posto λ ordinale e $Fun_\lambda = \{f : \lambda \longrightarrow \lambda\}$, allora per ogni monoide M esiste un ordinale μ tale che M si immerge in Fun_μ.*

Dimostrazione. Sia M monoide e sia $\succ$ ordinamento che rende $\mu = (M, \succ)$ ordinale, allora $\psi : M \longrightarrow Fun_\mu$ tale che $\psi(m)(a) = ma$ è un omomorfismo iniettivo, infatti: se $m \neq n$ allora $\psi(m)(e_M) = m \neq n = \psi(n)(e_M)$ quindi $\psi(m) \neq \psi(n)$, e $\psi(mn)(a) = mna = \psi(m)(na) = \psi(m)(\psi(n)(a)) = (\psi(m) \circ \psi(n))(a)$. □

Proposizione 1.7. *Sia M un monoide finito di cardnalità n, allora lo posso sempre immergere nello spazio delle matrici $M(n, \mathbb{C})$.*

Dimostrazione. M lo possiamo immergere nello spazio delle funzioni Fun_μ, inoltre per ogni $f \in Fun_\mu$ posso definire una mappa γ tale che sulla base canonica $\{e_i\}$ sia $\gamma(e_i) = e_{\tau(i)}$, dove posta una indicizzazione degli elementi di M, si ha che $f(a_i) = a_{\tau(i)}$. Tale γ si può estendere per linearità su tutto $\mathbb{C}^n$ ottenendo così una immersione di Fun_μ in $Mat(n, \mathbb{C})$ e quindi anche di M. (scrivere meglio) □

Esercizio 1. $(\mathbb{N} \setminus \{0\}, +) \times (\mathbb{Z}/_{6\mathbb{Z}}, \cdot)$ è completabile?

soluzione. Osserviamo che $(1, 0) * (1, 1) = (2, 0) = (1, 0)(1, 0)$. Se fosse estendibile allora $(1, 1) = (1, 0)^{-1}(1, 0) * (1, 1) = (1, 0)^{-1}(1, 0)(1, 0) = (1, 0)$ che è assurdo. □

Osservazione 1.30. L'esercizio precedente mostra un esempio di un semigruppo senza idempotenti e non estendibile, quindi nel caso di monoidi infiniti l'idempotenza non è un fattore sufficiente per l'estendibilità.

Osservazione 1.31. Col medesimo esempio si mostra che $(\mathbb{N} \setminus \{0\}, +) \times (\mathbb{Z}/_{n\mathbb{Z}}, \cdot)$ non è estendibile per ogni $n \in \mathbb{N}$.

Osservazione 1.32. Osserviamo inoltre che ogni monoide della forma $(\mathbb{N} \setminus \{0\}, +) \bigtimes_{i=1,\ldots,k} (\mathbb{Z}/_{n_i\mathbb{Z}}, \cdot)$ non è estendibile, infatti $(1, 0, \ldots, 0)(1, 1, \ldots, 0) = (1, 0, \ldots, 0)^2$ e si conclude come prima.

Osservazione 1.33. Osserviamo che i conti precedenti usano il fatto che gli $\mathbb{Z}/_{n\mathbb{Z}}$ hanno lo 0 che elemento distruttore, se lo togliessi cambierebbe qualcosa? consideriamo il sotto-semigruppo $(\mathbb{N}\setminus\{0\},+)\times(\{1,2,4\},\cdot)$ di $(\mathbb{N}\setminus\{0\},+)\times(\mathbb{Z}/_{6\mathbb{Z}},\cdot)$ e osserviamo che non è estendibile in quanto $(1,1)(1,4)=(2,4)=(1,4)(1,4)$ e si conclude per la stessa idea precedente. In questo caso avevo l'elemento neutro, dunque consideriamo il sotto-semigruppo $(\mathbb{N}\setminus\{0\},+)\times(\{2,4\},\cdot)$ sempre di $(\mathbb{N}\setminus\{0\},+)\times(\mathbb{Z}/_{6\mathbb{Z}},\cdot)$, e osserviamo che $(\{2,4\},\cdot)$ è un sotto-semigruppo di $(\mathbb{Z}/_{6\mathbb{Z}},\cdot)$ ma non è un suo sotto-gruppo, però è un gruppo isomorfo a $(\mathbb{Z}/_{2\mathbb{Z}},+)$, dunque trovo un isomorfismo tra $(\mathbb{N}\setminus\{0\},+)\times(\{2,4\},\cdot)$ e $(\mathbb{N}\setminus\{0\},+)\times(\mathbb{Z}/_{2\mathbb{Z}},+)$ e quest'ultimo lo posso immergere nel gruppo $(\mathbb{Z},+)\times(\mathbb{Z}/_{2\mathbb{Z}},+)$.

Esercizio 2. Classificare i monoidi di 3 elementi.

Soluzione. Sia M un monoide con 3 elementi, allora o è un gruppo, cioè $(\mathbb{Z}/_{3\mathbb{Z}},+)$, ho ha almeno un idempotente. Chiamiamo $M=\{e,a,b\}$ dove e è l'elemento neutro ed a un idempotente, allora si hanno tre possibilità per b^2: se $b^2=e$ allora $ab=ba=a$, infatti per esempio se $ab=b$ allora $a=ab^2=b^2=e$ assurdo, ottenendo dunque il monoide $(\mathbb{Z}/_{3\mathbb{Z}},\cdot)$. Negli altri due casi non può mai valere che $ab=e$ o $ba=e$, per esempio se $b^2=a$ allora $a=a^2=ab^2=b$ assurdo, dunque restringendo M a solo $\{a,b\}$ si ottengono anche tutti i semigruppi di 2 elementi che non sono estendibili. Abbiamo quindi 8 casi, ma il caso $b^2=b,\ ab=ba=a$ è isomorfo a $b^2=b,\ ab=ba=b$ con l'isomorfismo che scambia a con b, e i casi $a^2=b^2=a$ con $ab=a$ e $ba=b$ oppure $ab=b$ e $ba=a$ non sono possibili infatti se $b^2=a,\ ab=b$ e $ba=a$ allora $b=ab=b^3=ba=a$ che è assurdo. Quindi i restanti casi sono dati da:

$$a^2=ab=a \text{ e } b^2=ba=b \text{ è } < \begin{pmatrix}0&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\0&1\end{pmatrix} >;$$

$$a^2=ab=b^2=ba=a \text{ è } < \begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix} >;$$

$$a^2=b^2=a \text{ e } ab=ba=b \text{ è } < \begin{pmatrix}0&0\\0&1\end{pmatrix}, -\begin{pmatrix}0&0\\0&1\end{pmatrix} >;$$

$$a^2=ba=a \text{ e } b^2=ab=b \text{ è } < \begin{pmatrix}0&0\\1&1\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} >;$$

$$a^2=ab=ba=a \text{ e } b^2=b \text{ è } < \begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} >.$$

Questi elemencati sono tutti i semigruppi di due elementi non estendibili, che sono 5, contando quelli estendibili, cioè $(\mathbb{Z}/_{2\mathbb{Z}},+)$, sono in tutto 6, inoltre aggiungendo l'elemento neutro ai precedenti otteniamo i mancanti monoidi di 3 elementi, che con quelli contati precedentemenete sono in tutto 7. □

Osservazione 1.34. Siano M,N sotto-monoidi del monoide A tale che esiste $f:M\longrightarrow N$ isomorfismo, allora esiste $g:A\longrightarrow A$ isomorfismo tale che $g|_M=f$? No, infatti posto $A=(\mathbb{Z}/_{6\mathbb{Z}},\cdot)$, $M=\{1,3\}$ e $N=\{1,0\}$, allora M ed N sono isomorfi come monoidi ma non trovo un isomorfismo in $Aut(A)$ che estende quello tra M ed N, infatti un tale isomorfismo manda distruttore in distruttore cioè $g\in Aut(A)$ è tale che $g(0)=0$.

Definizione 1.23. Se trovo $g\in Aut(A)$ che estende $f:M\longrightarrow N$ isomorfismo tra sotto-monoidi di A, allora dico che M ed N sono $isomorfi\ come\ sotto-monoidi$.

Osservazione 1.35. E se M, N, A sono gruppi? Prima di tutti osserviamo che se $f : A \longrightarrow A$ è un isomorfismo, allora induce un isomorfismo tra lo stabilizzatore di $a \in A$ e $f(a)$, infatti: se $b \in Stab(a)$, allora $f(b)f(a)f(b)^{-1} = f(bab^{-1}) = f(a)$, cioè $f(b) \in Stab(f(a))$, se $c \in Stab(f(a))$ allora esiste $b \in A$ tale che $f(b) = c$, allora $f(a) = cf(a)c^{-1} = f(b)f(a)f(b)^{-1} = f(bab^{-1})$, e per iniettività $a = bab^{-1}$ dunque $b \in stab(a)$. Ora consideriamo $A = S_n$ con $n \geq 6$, $M =< (1, 2, 3) >$ e $N =< (1, 2, 3)(4, 5, 6) >$, allora M ed N sono isomorfi come gruppi ma non come sotto-gruppi in quanto i loro stabilizzatori non posso essere isomorfi per una questione di cardinalità.

Esercizio 3. $(\mathbb{Z}/_{nm\mathbb{Z}}, \cdot) \cong (\mathbb{Z}/_{n\mathbb{Z}}, \cdot) \times (\mathbb{Z}/_{m\mathbb{Z}}, \cdot)$.

Soluzione. Consideriamo la mappa $\gamma : (\mathbb{Z}/_{nm\mathbb{Z}}, \cdot) \longrightarrow (\mathbb{Z}/_{n\mathbb{Z}}, \cdot) \times (\mathbb{Z}/_{m\mathbb{Z}}, \cdot)$ tale che $\gamma([a]_{nm}) = ([a]_n, [a]_m)$, è un omomorfismo iniettivo, infatti: $\gamma([ab]_{nm}) = ([ab]_n, [ab]_m) = ([a]_n[b]_n, [a]_m[b]_m) = ([a]_n, [a]_m)([b]_n, [b]_m) = \gamma([a]_{nm})\gamma([b]_{nm})$, e se $a \equiv b\ (n)$ e $a \equiv b\ (m)$ per il Teorema cinese del resto vale che $a \equiv b\ (nm)$. Infine siccome $(\mathbb{Z}/_{nm\mathbb{Z}}, \cdot)$ e $(\mathbb{Z}/_{n\mathbb{Z}}, \cdot) \times (\mathbb{Z}/_{m\mathbb{Z}}, \cdot)$ hanno la stessa cardinalità, allora γ è un isomorfismo. $\square$

Definizione 1.24. Sia M un monoide con zero. Posto a lo zero di M dico che $b \in M$ è *nilpotente* se esiste $n \in \mathbb{N}$ tale che $b^n = a$.