UNIVERSITÀ DEGLI STUDI DI CATANIA
Dipartimento di matematica e informatica
corso di laurea triennale in Matematica

Alessio Borzì

SEMIGRUPPI DI ARF E DUPLICAZIONE NUMERICA

Elaborato di Laurea

Relatore:
Chiar.mo Prof. M. D'Anna

anno accademico 2016/2017

Indice

Introduzione

Il matematico F.G. Frobenius durante le sue lezioni poneva il seguente problema: trovare una formula per calcolare il più grande intero che non si può scrivere come combinazione lineare a coefficienti interi non negativi di un insieme di interi positivi con massimo comune divisore uguale a 1.
Questo problema, noto come problema delle monete, o problema di Frobenius, equivale a determinare il massimo intero N che non sia soluzione dell'equazione lineare diofantea

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = N$$

con coefficienti a_i non negativi, $MCD(x_1, x_2, \ldots, x_n) = 1$ e $x_i > 0$ ed esprimere N in funzione di $x_1, x_2, \ldots, x_n$.
Nel caso particolare $n = 2$ il problema è stato risolto nel 1884 da Sylvester [9] e si ha, come vedremo nella Proposizione 1.1.24, $N = x_1x_2 - x_1 - x_2$. Il caso generale è notevolmente più complicato. Infatti per $n \geq 3$ non esiste una formula polinomiale che esprima N in funzione dei di $x_1, x_2, \ldots, x_n$ (si veda [4]).

Lo studio dei semigruppi numerici (cioè dei sottomonoidi di $\mathbb{N}$ con complementare finito) nasce nell'ambito della teoria dei numeri e trova una delle sue motivazioni nel problema di Frobenius. I semigruppi numerici hanno però molte altre applicazioni, ad esempio nell'algebra commutativa e nella teoria delle singolarità delle curve.

O. Zariski, nel primo dei suoi tre lavori sulle equisingolarità [10], introdusse una classificazione delle singolarità delle curve affini irriducibili attraverso la loro successione di molteplicità. Più tardi J. Lipman [6], ispirato da un lavoro di C. Arf [1], introdusse una nuova classe di anelli, gli anelli di Arf e la nozione di "chiusura di Arf" di un anello A, ossia il più piccolo anello di Arf che contiene A. Tramite il semigruppo numerico associato alla chiusura di Arf dell'anello associato alla curva è possibile risalire alla successione delle molteplicità.
Dalla nozione di anello di Arf, considerando il suo semigruppo numerico associato, nasce la nozione di semigruppo numerico di Arf. Diverse proprietà di questa classe di semigruppi numerici sono state studiate in [2] e [8].

In questa tesi vengono presentati i semigruppi numerici e i semigruppi di Arf (capitolo 1) e viene studiata la proprietà di Arf su una particolare costruzione, ovvero la duplicazione numerica, introdotta in [5] (capitolo 2).
Nella prima sezione del primo capitolo si definiscono i semigruppi numerici e vengono date, in riferimento a quanto fatto in [7], alcune nozioni principali come la molteplicità, la dimensione d'immersione o il numero di Frobenius. Si mostra che ogni sottomonoide di $(\mathbb{N}, +)$ è isomorfo a un semigruppo numerico e che ogni semigruppo numerico possiede un unico sistema minimale di

generatori finito.
Nella seconda sezione vengono trattati brevemente i semigruppi numerici simmetrici, riportandone una classica caratterizzazione.
Nella terza sezione vengono presentati, in analogia con la teoria degli anelli, gli ideali di semigruppo numerico, ripercorrendo quanto fatto in [2]. Viene introdotto il semigruppo di Lipman, ossia l'equivalente numerico del blow-up definito in [6]. Si dà la nozione di ideale stabile, studiandone alcune proprietà principali.
Nella quarta sezione vengono trattati brevemente i semigruppi numerici di dimensione d'immersione massima, cioè i semigruppi numerici con dimensione d'immersione pari alla molteplicità. I semigruppi di Arf sono una particolare classe di questo tipo di semigruppi numerici.
Nella quinta sezione si studiano i semigruppi numerici di Arf dandone due definizioni equivalenti. Seguendo quanto fatto in [2], si introduce il blow-up di un semigruppo numerico e le tre catene S_i, L_i e B_i associate a un semigruppo numerico. Viene introdotta la nozione di chiusura di Arf di un semigruppo numerico. Si definisce la successione di molteplicità di un semigruppo numerico e si mostra che il blow-up commuta con la chiusura di Arf. Un'importante conseguenza di quest'ultimo fatto è che un semigruppo numerico e la sua chiusura di Arf hanno la stessa successione di molteplicità. Infine, vengono caratterizzate le cosiddette "successioni di Arf", cioé successioni di interi che sono successioni di molteplicità di qualche semigruppo numerico.
Nella prima sezione del capitolo due viene presentata la duplicazione numerica e alcune delle sue proprità in relazione al quoziente di un semigruppo numerico e alla simmetria, riportando quanto sviluppato in [5].
Nella seconda e ultima sezione della tesi vengono fatte alcune osservazioni e dimostrati alcuni risultati che legano la proprietà di Arf e la duplicazione numerica. In particolare, viene proposta una caratterizzazione delle duplicazioni numeriche che hanno la proprietà di Arf e che sono costruite a partire da un semigruppo di Arf.

Capitolo 1

Semigruppi Numerici

In questo capitolo introduciamo alcune definizioni e risultati fondamentali riguardanti la teoria dei semigruppi numerici.

1.1 Prime definizioni

Definizione 1.1.1. *Sia S un insieme e $+$ un'operazione binaria interna su S. Se $+$ è associativa allora coppia $(S,+)$ si dice **semigruppo**.*

Definizione 1.1.2. *Sia $(S,+)$ un semigruppo. Se esiste un elemento $0 \in S$ tale che $0+a = a+0 = a$ per ogni $a \in S$ allora $(S,+)$ è detto **monoide**. L'elemento $0 \in S$ è detto **elemento neutro**.*

L'elemento neutro di un monoide $(S,+)$ è unico. Infatti se 0 e $0'$ sono due elementi neutri di S allora

$$0 = 0 + 0' = 0' \Rightarrow 0 = 0'.$$

Definizione 1.1.3. *Se l'operazione di un semigruppo (o monoide) $(S,+)$ è commutativa allora il semigruppo (risp. monoide) è detto **commutativo**.*

Definizione 1.1.4. *Sia $(S,+)$ un semigruppo. Un sottoinsieme $T \subseteq S$ chiuso rispetto a $+$ (cioè tale che $a+b \in T$ per ogni $a,b \in T$) è detto **sottosemigruppo** di S.*

Definizione 1.1.5. *Sia $(S,+)$ un monoide. Un sottoinsieme $T \subseteq S$ chiuso rispetto a $+$ con $0 \in T$ è detto **sottomonoide** di S.*
*I due sottomonoidi $\{0\}$ ed S di $(S,+)$ sono detti **sottomonoidi banali**.*

È facile verificare che l'intersezione di due sottomonoidi (o di due sottosemigruppi) è ancora un sottomonoide (risp. un sottosemigruppo).

Dato un monoide $(S,+)$ e un sottoinsieme $A \subseteq S$ l'intersezione di tutti i sottomonoidi di S contenenti A è l'insieme

$$\langle A \rangle = \{\lambda_1 a_1 + \ldots + \lambda_n a_n : n \in \mathbb{N}, \lambda_1, \ldots, \lambda_n \in \mathbb{N}, a_1, \ldots, a_n \in A\}$$

(dove, se $a \in A$ e $n \in \mathbb{N}$, intendiamo $na = \underbrace{a + \ldots + a}_{n \text{ volte}}$, con $0a = 0 \in S$).

Ovviamente $\langle A \rangle$ è il più piccolo sottomonoide di S contenente A ed è detto sottomonoide di

S generato da A. Nel caso di un insieme finito $A = \{a_1, a_2, \ldots, a_n\}$ scriveremo con abuso di notazione $\langle A \rangle = \langle a_1, a_2, \ldots, a_n \rangle$ e diremo che $\langle A \rangle$ è **finitamente generato** e che $\{a_1, a_2, \ldots, a_n\}$ è un **sistema di generatori** per $\langle A \rangle$.

In base alle definizioni precedenti $(\mathbb{N}, +)$ risulta un monoide commutativo. Siamo adesso pronti per dare la definizione di semigruppo numerico.

Definizione 1.1.6. *Un sottomonoide S di $(\mathbb{N}, +)$ è detto* ***semigruppo numerico*** *(abbreviato s.n.) se l'insieme $\mathbb{N} \setminus S$ è finito.*

Esempio 1.1.7. L'insieme dei numeri pari $2\mathbb{N} \subseteq \mathbb{N}$ è un sottomonoide di $(\mathbb{N}, +)$ ma non è un semigruppo numerico in quanto il suo complementare in $\mathbb{N}$ corrisponde all'insieme dei numeri dispari che non è un insieme finito.
Invece l'insieme $S = \langle 2, 3 \rangle = \{0, 2, 3, \rightarrow\}$ (dove il simbolo $\rightarrow$ indica che tutti i numeri maggiori o uguali all'ultimo elemento elencato, il 3, appartengono ad S) è un semigruppo numerico, infatti com'è facile verificare è un sottomonoide di $(\mathbb{N}, +)$ e il suo complementare $\mathbb{N} \setminus S = \{1\}$ è un insieme finito.

Dato $A \subseteq \mathbb{Z}$ un sottoinsieme non vuoto, possiamo considerare in $\mathbb{Z}$ l'ideale $I \subseteq \mathbb{Z}$ generato da A (cioè l'intersezione di tutti gli ideali di $\mathbb{Z}$ che contengono A). Dal momento che $\mathbb{Z}$ è un PID avremo che $I = (d)$ con $d \in \mathbb{N}$. Poniamo $\mathrm{MCD}(A) = d$. Osserviamo che d è il più grande numero positivo che divide tutti gli elementi di $\langle A \rangle$.

Lemma 1.1.8. [7, Lemma 2.1] *Sia $A \subseteq \mathbb{N}$ un sottoninsieme non vuoto. Il sottomonoide $\langle A \rangle$ è un semigruppo numerico se e solo se $MCD(A) = 1$.*

Dimostrazione.

- $\Rightarrow$ Sia $d = MCD(A)$. Dato che $\mathbb{N} \setminus \langle A \rangle$ è un insieme finito esiste $x \in \mathbb{N}$ tale che $x, x+1 \in \langle A \rangle$, da cui d divide sia x che $x+1$ quindi $d = 1$.

- $\Leftarrow$ Proviamo che $\mathbb{N} \setminus \langle A \rangle$ è finito. Per ipotesi $\mathrm{MDC}(A) = 1$ quindi esistono $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ e $a_1, a_2, \ldots, a_n \in A$ tali che $z_1 a_1 + \ldots + z_n a_n = 1$. Portando i termini con coefficienti z_i negativi a secondo membro scriviamo

$$z_{i_1} a_{i_1} + \ldots + z_{i_k} = 1 - z_{j_1} a_{j_1} - \ldots - z_{j_t} a_{j_t}.$$

Dunque abbiamo trovato un elemento $s \in \langle A \rangle$ tale che $s + 1 \in \langle A \rangle$. Proviamo adesso che ogni $n \geq (s-1)(s+1) = (s-1)s + (s-1)$ appartiene a $\langle A \rangle$. Siano $q, r \in \mathbb{N}$ tali che $n = qs + r$ con $0 \leq r \leq s-1$. Dal fatto che $n \geq (s-1)s + (s-1)$ deduciamo che $q \geq s-1 \geq r$, quindi possiamo scrivere

$$n = (q-r)s + rs + r = (q-r)s + r(s+1) \in \langle A \rangle.$$ □

Definizione 1.1.9. *Siano $(X, +)$,$(Y, *)$ due semigruppi.*
Una funzione $f : X \rightarrow Y$ tale che

$$f(a+b) = f(a) * f(b) \quad \forall a, b \in X$$

è detta ***omomorfismo*** *di semigruppi. Se f è biiettiva allora è detta* ***isomorfismo*** *di semigruppi.*

Definizione 1.1.10. *Siano $(X, +)$,$(Y, *)$ due monoidi. Un omomorfismo $f : X \rightarrow Y$ di semigruppi tale che $f(0_X) = 0_Y$ è detto* ***omomorfismo*** *di monoidi (dove 0_X e 0_Y sono rispettivamente gli elementi neutri di X e Y). Se f è biiettivo allora è detto* ***isomorfismo*** *di monoidi.*

Definizione 1.1.11. *Due monoidi (o semigruppi) X e Y si dicono* ***isomorfi*** *se esiste un isomorfismo di monoidi (risp. semigruppi) $f : X \to Y$.*

Il prossimo risultato mostra come i semigruppi numerici classificano, a meno di isomorfismi, i sottomonoidi di $\mathbb{N}$.

Proposizione 1.1.12. [7, Proposition 2.2] *Se M è un sottomonoide non banale di $\mathbb{N}$ allora esso è isomorfo a un semigruppo numerico.*

Dimostrazione. Sia $d = MCD(M)$. Dal Lemma 1.1.8 sappiamo che $S = \{\frac{m}{d} : m \in M\}$ è un semigruppo numerico. L'applicazione $f : M \to S$ con $f(m) = \frac{m}{d}$ è chiaramente un isomorfismo di monoidi. $\square$

Se A e B sono due sottoinsiemi di $\mathbb{Z}$ scriviamo $A + B = \{a + b : a \in A, b \in B\}$.
Se S è un sottomonoide di $\mathbb{N}$ scriviamo $S^* = S \setminus \{0\}$.

Lemma 1.1.13. [7, Lemma 2.3] *Se S è un sottomonoide di $\mathbb{N}$ allora $S^* \setminus (S^* + S^*)$ è il minimo (rispetto all'inclusione) sistema di generatori di S.*

Dimostrazione. Dobbiamo provare che $S^* \setminus (S^* + S^*)$ è un sistema di generatori per S e che ogni altro sistema di generatori per S contiene $S^* \setminus (S^* + S^*)$.
Sia $s \in S^*$. Se $s \notin S^* \setminus (S^* + S^*)$ allora esistono $x, y \in S^*$ tali che $s = x + y$. Ripetendo il procedimento per x e y, dopo un numero finito di passaggi (dato che $x, y < s$) troviamo $s_1, \ldots, s_n \in S^* \setminus (S^* + S^*)$ tali che $s = s_1 + \ldots + s_n$. Questo prova che $S^* \setminus (S^* + S^*)$ è un sistema di generatori per S.
Sia adesso A un sistema di generatori per S. Sia $x \in S^* \setminus (S^* + S^*)$. Per ipotesi esistono $n \in \mathbb{N}, \lambda_1, \ldots, \lambda_n \in \mathbb{N}$ e $a_1, \ldots, a_n \in A$ tali che $x = \lambda_1 a_1 + \ldots + \lambda_n a_n$. Dato che $x \notin S^* + S^*$ si ha $x = a_i$ per qualche $i \in \{1, \ldots, n\}$. $\square$

Definizione 1.1.14. *Sia S un semigruppo numerico e sia $n \in S^*$. Si definisce* ***insieme di Apéry*** *di n in S come segue*

$$\mathrm{Ap}(S, n) = \{s \in S : s - n \notin S\}.$$

Lemma 1.1.15. [7, Lemma 2.4] *Se S è un semigruppo numerico e $n \in S^*$, allora $\mathrm{Ap}(S, n) = \{0 = w(0), w(1), \ldots, w(n-1)\}$, dove $w(i)$ è il più piccolo elemento di S congruo a i modulo n, per ogni $i \in \{0, \ldots, n-1\}$.*

Dimostrazione. Basta osservare che per ogn $i \in \{0, \ldots, n-1\}$, esiste $k \in \mathbb{N}$ tle che $i + kn \in S$. $\square$

Corollario 1.1.16. *Se S è un semigruppo numerico e $n \in S^*$, allora $\mathrm{Ap}(S, n)$ è un insieme finito di cardinalità n.*

Corollario 1.1.17. [7, Lemma 2.6] *Se S è un semigruppo numerico e $n \in S^*$, allora l'insieme $(\mathrm{Ap}(S, n) \setminus \{0\}) \cup \{n\}$ è un sistema di generatori per S.*

Dimostrazione. Basta osservare che per ogni $s \in S^*$ congruo a i modulo n esiste $k \in \mathbb{N}$ tale che $s = kn + w(i)$. $\square$

Teorema 1.1.18. [7, Theorem 2.7] *Ogni semigruppo numerico S possiede un unico sistema di generatori minimale finito.*

Dimostrazione. Dal Lemma 1.1.13 sappiamo che $S^* \setminus (S^* + S^*)$ è l'unico sistema minimale di generatori che, in base al Corollario 1.1.17, è contenuto nell'insieme $(\mathrm{Ap}(S, n) \setminus \{0\}) \cup \{n\}$ (con $n \in S^*$). Quest'ultimo è un insieme finito in base al Corollario 1.1.16. $\square$

Dato un semigruppo numerico S, su $\mathbb{Z}$ possiamo introdurre la seguente relazione d'ordine parziale

$$a \leq_S b \Longleftrightarrow a - b \in S.$$

In questo modo, in base al teorema precedente, i geneatori di S non sono altro che gli elementi minimali di $S \setminus \{0\}$ rispetto a $\leq_S$.

Definizione 1.1.19. *Sia S un semigruppo numerico e $\{n_1 < n_2 < \ldots < n_p\}$ il suo sistema minimale di generatori. Definiamo **molteplicità** di S l'elemento n_1 e sarà indicata con $m(S)$, mentre la **dimensione d'immersione** di S corrisponde a p, cioè il numero di generatori minimale, e sarà indicata con $ed(S)$.*

D'ora in avanti, quando non specificheremo rispetto a quale elemento calcoliamo l'insieme di Apéry, intenderemo sempre rispetto alla molteplicità del semigruppo. In questo modo indichiamo $\mathrm{Ap}(S) = \mathrm{Ap}(S, m(S))$.

Proposizione 1.1.20. [7, Proposition 2.10] *Sia S un semigruppo numerico.*

1. $m(S) = \min(S \setminus \{0\})$,
2. $ed(S) \leq m(S)$.

Dimostrazione. Il primo punto è banale. Per il secondo punto basta osservare che l'insieme $(\mathrm{Ap}(S) \setminus \{0\}) \cup \{m(S)\}$ è un sistema di generatori di cardinalità $m(S)$. □

Definizione 1.1.21. *Sia S un semigruppo numerico. Si definisce **numero di Frobenius** di S il numero $F(S) = \max(\mathbb{N} \setminus S)$. Si definisce **genere** di S il numero $g(S) = |\mathbb{N} \setminus S|$. Si definisce **conduttore** di S il numero $c(S) = F(S) + 1$. Indichiamo con $N(S) = \{x \in S : x < F(S)\}$ e con $n(S) = |N(S)|$.*

Osserviamo che ogni intero maggiore o uguale del conduttore appartiene al semigruppo numerico.

Bras-Amorós in [3] ha calcolato il numero n_g di semigruppi numerici di un dato genere g per $g \in \{0, \ldots, 50\}$. I suoi calcoli mostrano che la successione n_g ha un comportamento molto simile alla successione di Fibonacci.

Osservazione 1.1.22. [7, Lemma 2.14] Sia S un semigruppo numerico. Osserviamo che se $x \in S$ allora $F(S) - x \notin S$, altrimenti $F(S) = x + (F(S) - x) \in S$, assurdo. Equivalentemente abbiamo $F(S) - x \in S \Rightarrow x \in \mathbb{Z} \setminus S$. In altri termini deduciamo che $n(S) \leq g(S)$. Inoltre dato che si ha $n(S) + g(S) = F(S) + 1$ otteniamo

$$2g(S) \geq n(S) + g(S) = F(S) + 1 \Rightarrow g(S) \geq \frac{F(S) + 1}{2}$$

Proposizione 1.1.23. [7, Proposition 2.12] *Sia S un semigruppo numerico e $n \in S^*$.*

1. $F(S) = \max(\mathrm{Ap}(S, n)) - n$,
2. $g(S) = \frac{1}{n} \left(\sum_{w \in \mathrm{Ap}(S,n)} w \right) - \frac{n-1}{2}$.

Dimostrazione.

1. Dalla definizione sappiamo che $F(S) + n \in \mathrm{Ap}(S, n)$. Se per assurdo esiste $w \in \mathrm{Ap}(S, n)$ tale che $w > F(S) + n$ allora $w - n > F(S)$ con $w - n \in \mathbb{N} \setminus S$, assurdo.

2. Osserviamo che per ogni $w \in \mathrm{Ap}(S,n)$ se w è congruo a i modulo n allora esiste $k_i \in \mathbb{N}$ tale che $w = k_i n + i$. In questo modo, con la stessa notazione utilizzata in precedenza, abbiamo $w(i) = k_i n + i$ al variare di $i \in \{0, \ldots, n-1\}$. Adesso, ogni intero x congruo a i modulo n appartiene a S se e solo se $w(i) \leq x$. Dunque abbiamo

$$\begin{aligned} g(S) &= k_1 + \ldots + k_{n-1} = \\ &= \frac{1}{n}\Big((k_1 n + 1) + \ldots + (k_{n-1}n + n - 1)\Big) - \frac{n-1}{2} = \\ &= \frac{1}{n}\left(\sum_{w \in \mathrm{Ap}(S,n)} w\right) - \frac{n-1}{2}. \end{aligned}$$

□

Proposizione 1.1.24. [7, Proposition 2.13] *Se $a, b \in \mathbb{N}$ con $MCD(a,b) = 1$ allora abbiamo $F(\langle a, b\rangle) = ab - a - b$.*

Dimostrazione. Basta utilizzare il risultato precedente una volta osservato che

$$\mathrm{Ap}(\langle a, b\rangle, a) = \{0, b, 2b, \ldots, (a-1)b\}.$$

□

1.2 Semigruppi simmetrici

Introduciamo brevemente in questa sezione la classe dei semigruppi simmetrici.

Definizione 1.2.1. *Sia S un semigruppo numerico. Un intero $x \in \mathbb{Z}$ è un numero **pseudo-Frobenius** se $x \notin S$ e $x+s \in S$ per ogni $s \in S \setminus \{0\}$. L'insieme dei numeri pseudo-Frobenius viene indicato con $PF(S)$. La cardinalità di tale insieme viene detta **tipo** del semigruppo numerico e viene indicata con $t(S)$.*

Osserviamo che per ogni semigruppo numerico S si ha $F(S) \in PF(S)$, quindi anche $t(S) \geq 1$.

Definizione 1.2.2. *Un semigruppo numerico S è detto **simmetrico** se $PF(S) = \{F(S)\}$ (o equivalentemente $t(S) = 1$). S viene detto **pseudo-simmetrico** se $PF(S) = \{F(S), \frac{F(S)}{2}\}$.*

Osservazione 1.2.3. Osserviamo che $PF(S) = \mathrm{Massimali}_{\leq_S}(\mathbb{Z} \setminus S)$. Infatti sia $x \in PF(S)$, se per assurdo esistesse $y \in \mathbb{Z} \setminus S$ tale che $x \leq_S y$, cioè $y - x \in S$, allora $x + (y-x) = y \notin S$, contraddicendo il fatto che $x \in PF(S)$, assurdo (si veda [7, Proposition 2.19]).

Dall'osservazione precedente e dall'Osservazione 1.1.22 otteniamo facilmente il seguente risultato

Proposizione 1.2.4. *Per un semigruppo numerico S sono equivalenti*

1. *S è simmetrico.*
2. *$F(S) = \max_{\leq_S}(\mathbb{Z} \setminus S)$.*
3. *$x \in \mathbb{Z} \setminus S \Leftrightarrow F(S) - x \in S$.*
4. *$f : S \to \mathbb{Z} \setminus S$ con $f(x) = F(S) - x$ è una biizione.*
5. *$\mathbb{Z} = S \cup (F(S) - S)$.*
6. *$g(S) = \frac{F(S)+1}{2}$.*

(ad esempio si veda [7, Proposition 4.4] e [7, Corollary 4.5])

1.3 Ideali Stabili

Diamo adesso alcune nozioni introdotte da J. Lipman in [6], presentandole dal punto di vista dei semigruppi numerici similmente a quanto fatto in [2].

Dati $z \in \mathbb{Z}$ e $A \subseteq \mathbb{Z}$ con la scrittura $z + A$ intendiamo l'insieme $\{z + a : a \in A\}$. Se $z \in \mathbb{N}$ con la scrittura zA intendiamo $\underbrace{A + A + \ldots + A}_{z \text{ volte}}$, con $0A = \{0\}$.

Definizione 1.3.1. *Sia S un semigruppo numerico. Un **ideale relativo** di S è un insieme $I \subseteq \mathbb{Z}$ tale che $S + I \subseteq I$ e $s + I \subseteq S$ per qualche $s \in S$ (o equivalentemente I possiede un minimo). Un ideale relativo di S che è contenuto in S verrà chiamato semplicemente **ideale** di S. Ogni ideale relativo del tipo $x + S$ con $x \in \mathbb{Z}$ è chiamato **ideale principale relativo**, o semplicemente **ideale principale** se è contenuto in S.*

È facile verificare che se $I, J \subseteq \mathbb{Z}$ sono due ideali relativi di un semigruppo numerico S allora lo sono anche $I + J$, $I \cap J$, $I - J = \{z \in \mathbb{Z} : z + J \subseteq I\}$.

Dato un semigruppo numerico S e un insieme $A \subseteq S$, l'intersezione di tutti gli ideali di S contenenti A è l'insieme $I = A + S$ ed esso è il più piccolo ideale di S contenente A. Nel caso di un insieme finito $A = \{a_1, \ldots, a_n\}$ diremo che l'ideale I è **finitamente generato** e scriveremo $I = (a_1, \ldots, a_n) + S$.

Osserviamo che ogni ideale I di un semigruppo numerico S è finitamente generato. Infatti $I \cup \{0\}$ può essere visto a sua volta come un semigruppo numerico ($I + I \subseteq S + I \subseteq I$).
Il sistema minimale di generatori di I (come ideale di S) coincide con l'insieme degli elementi minimali rispetto alla relazione $\leq_S$ su I. In generale questo insieme è contenuto (anche strettamente) nell'insieme minimale di generatori di $I \cup \{0\}$ visto come semigruppo numerico.

Esempio 1.3.2. Sia $S = \langle 2, 3 \rangle = \{0, 2, 3, \rightarrow\}$ e $I = 3 + \mathbb{N} = \{3, \rightarrow\}$. Abbiamo $I = (3, 4) + S$ mentre $I \cup \{0\} = \langle 3, 4, 5 \rangle$.

Definizione 1.3.3. *Sia S un semigruppo numerico. Un ideale I di S si dice **proprio** se $I \subsetneq S$. L'**ideale massimale** di S è $M = S \setminus \{0\} = S^*$.*

In analogia alla terminologia usata nella teoria degli anelli, ogni ideale proprio di S è contenuto nell'ideale massimale M.
È facile verificare che $M - M = S - M$. Inoltre osserviamo che con le notazioni introdotte $(M - M) \setminus S = PF(S)$.

Proposizione 1.3.4. *Sia S un semigruppo numerico e I un suo ideale. Per ogni intero $n \geq 1$ si ha*

1. *$nI - nI \subseteq (n + 1)I - (n + 1)I$*
2. *$nI - nI$ è un semigruppo numerico contenente S.*

Dimostrazione.

1. Sia $x \in nI - nI$, per ogni $y \in (n + 1)I$ possiamo scrivere $y = i + j$ con $i \in I$ e $j \in nI$. Si ha $x + y = (x + j) + i \in nI + I = (n + 1)I$, da cui $x \in (n + 1)I - (n + 1)I$.

2. Chiaramente $nI - nI \subseteq \mathbb{N}$. Infatti se per assurdo esistesse $x \in nI - nI$ con $x < 0$, detto $i = \min(nI)$, avremmo $x + i < i$ dunque $x + i \notin nI$, assurdo.
   Siano $x, y \in nI - nI$ e $i \in nI$. Per ipotesi si ha $y+i \in nI$ da cui $(x+y)+i = x+(y+i) \in nI$, cioè $x + y \in nI - nI$.
   Sia adesso $s \in S$ e $i \in nI$, allora $s + i \in S + nI \subseteq nI$, quindi $s \in nI - nI$. Pertanto $S \subseteq nI - nI$, da cui $\mathbb{N} \setminus (nI - nI) \subseteq \mathbb{N} \setminus S$. Ne segue che $nI - nI$ è un semigruppo numerico. □

In base alla proposizione precedente si viene a creare la seguente catena di semigruppi numerici

$$S \subseteq I - I \subseteq \ldots \subseteq nI - nI \subseteq (n+1)I - (n+1)I \subseteq \ldots \subseteq \mathbb{N}.$$

La precedente catena deve essere una catena ascendente finita, in quanto per ipotesi $\mathbb{N} \setminus S$ è un insieme finito. Pertanto deve esistere $r \in \mathbb{N}$ tale che

$$rI - rI = nI - nI \quad \forall n \geq r.$$

Il numero $r = r(I) \in \mathbb{N}$ è detto **numero di riduzione** di I.

Definizione 1.3.5. *Sia S un semigruppo numerico e I un suo ideale. Si definisce* ***semigruppo di Lipman*** *di S rispetto a I*

$$L(S, I) = \bigcup_{n \geq 1} nI - nI.$$

In base a quanto detto prima, se $r = r(I)$ risulta

$$L(S, I) = rI - rI.$$

Proposizione 1.3.6. [2, Proposition 1.2.1] *Sia S un semigruppo numerico e I un suo ideale con $i_1 = \min I$. Si ha*

1. $L(S, I) = \{z - ki_1 : z \in kI, k \geq 1\} = \bigcup_{k \geq 1}(kI - ki_1)$,
2. $(h + 1)I = hI + i_1$ *per ogni* $h \geq r(I)$.

Dimostrazione.

1. Proviamo prima che $(h + 1)I = hI + i_1$ per qualche $h \geq 1$. Per ogni $j \geq 1$ consideriamo l'insieme $B_j = \{x \in \mathbb{N} : x \geq ji_1, x \notin jI\}$. Dato che jI è un ideale di S si ha $jI + S \subseteq jI$ e quindi jI deve contenere tutti gli interi da un certo punto in poi, pertanto $|B_j| = b_j$ è finita. Inoltre $b_j \geq b_{j+1}$ in quanto l'applicazione $f_j : B_{j+1} \to B_j$ con $f(x) = x - i_1$ è iniettiva. Quindi esiste un $h \geq 1$ tale che $b_{h+1} = b_h$. Supponiamo per assurdo che esista $\alpha \in (h + 1)I \setminus (hI + i_1)$. Poiché $\alpha \in (h + 1)I$ allora $\alpha \geq (h + 1)i_1$; inoltre $\alpha \notin hI + i_1$ implica che $\alpha - i_1 \notin hI$, da cui $\alpha - i_1 \in B_h = f_h(B_{h+1})$. Ne segue che $\alpha - i_1 = f_h(\beta) = \beta - i_1 \Rightarrow \alpha = \beta \in B_{h+1}$, quindi $\alpha \notin (h + 1)I$, assurdo. Pertanto $(h + 1)I \subseteq hI + i_1$, l'altra inclusione è banale.
   Se $x \in L(S, I)$ allora $x \in kI - kI$ per qualche $k \geq 1$. Poniamo $z = x + ki_1 \in kI$, quindi $x = z - ki_1$, cioè $L(S, I) \subseteq \bigcup_{k \geq 1}(kI - ki_1)$. Viceversa sia $x = z - ki_1$ con $k \geq 1$ e $z \in kI$. Da $(h+1)I = hI + i_1$ per qualche $h \geq 1$ segue facilmente per induzione che $(h+k)I = hI + ki_1$. Quindi
   $$x + (h + k)I = z - ki_1 + hI + ki_1 = z + hI \subseteq (h + k)I,$$
   cioè $x \in (h + k)I - (h + k)I \subseteq L(S, I)$.

2. Se $h \geq r(I)$ allora $L(S,I) = hI - hI$, quindi $hI - hI = \bigcup_{k\geq 1}(kI - ki_1)$. Pertanto $I - i_1 \subseteq hI - hI$, da cui $(h+1)I \subseteq hI + i_1$, l'inclusione inversa è banale. □

Definizione 1.3.7. *Un ideale I di S è **stabile** se $r(I) = 1$ (o equivalentemente se $L(S,I) = I - I$).*

Corollario 1.3.8. [2, Corollary 1.2.3] *Sia S un semigruppo numerico, I un suo ideale e sia i_1 il minimo di I. Le seguenti proprietà sono equivalenti per I.*

1. *I è stabile.*
2. *$2I = I + i_1$.*
3. *$|I \setminus 2I| = i_1$.*
4. *$I - I = I - i_1$.*
5. *$I - i_1$ è un semigruppo numerico.*

Dimostrazione.

- (1) ⇒ (2) Segue dal punto 2 della proposizione precedente con $h = 1$.
- (2) ⇔ (3) Ogni elemento $x \in I \setminus I + i_1$ è tale che $x - i_1 \notin I$, cioè ogni elemento di $I \setminus I + i_1$ è minimale nella sua classe di resto modulo i_1 tra tutti gli elementi di hI. Dato che $hI + S \subseteq hI$ e da un certo punto in poi S contiene tutti gli interi, ciascuna di queste classi di resto è rappresentata in I, pertanto $|I \setminus I + i_1| = i_1$. Infine, da $I + i_1 \subseteq 2I \subseteq I$ si ha l'equivalenza.
- (2) ⇒ (4) Sia $x \in I - I$ allora $x + i_1 \in I$ da cui $x \in I - i_1$. Viceversa sia $x = y - i_1 \in I - i_1$ con $y \in I$ e sia $z \in I$. Si ha

  $$x + z = y + z - i_1 \in 2I - i_1 = (I + i_1) - i_1 = I,$$

  da cui $x \in I - I$.
- (4) ⇒ (5) Ovvio in base al punto 2 della Proposizione 1.3.4.
- (5) ⇒ (2) Siano $x, y \in I$, per ipotesi $(x - i_1) + (y - i_1) = z - i_1 \in I - i_1$, da cui $x + y = z + i_1 \in I + i_1$, cioè $2I \subseteq I + i_1$. L'altra inclusione è banale.
- (2)+(4) ⇒ (1) Dimostriamo per induzione su k che $kI - ki_1 = I - i_1$. La base dell'induzione è verificata per ipotesi. Supponiamo che $kI - ki_1 = I - i_1$, allora

  $$(k+1)I - (k+1)i_i = I + (kI - ki_1) - i_1 = 2I - 2i_1 = I - i_1.$$

  Dal punto 1 della proposizione precedente abbiamo $L(S,I) = I - i_1 = I - I$, cioè I è stabile. □

1.4 Dimensione d'immersione massima

Definizione 1.4.1. *Un semigruppo numerico S è di **dimensione d'immersione massima** se $ed(S) = m(S)$.*

Proposizione 1.4.2. [7, Proposition 3.1] *Se S è un semigruppo numerico S e $\{n_1 < \ldots < n_e\}$ è il suo sistema di generatori minimale allora S è di dimensione d'immersione massima se e solo se $Ap(S) = \{0, n_2, \ldots, n_e\}$.*

Dimostrazione. Basta osservare che $\{n_1, n_2, \ldots, n_e\} \subseteq (\mathrm{Ap}(S) \setminus \{0\}) \cup \{n_1\}$. Infatti la cardinalità di $\mathrm{Ap}(S)$ è n_1, pertanto $e = n_1$ se e solo se $\mathrm{Ap}(S) = \{0, n_2, \ldots, n_e\}$. □

Corollario 1.4.3. [7, Corollary 3.2] *Sia S un semigruppo numerico e $\{n_1 < n_2 < \ldots < n_e\}$ il suo sistema minimale di generatori. Se S è di dimensione d'immersione massima allora $F(S) = n_e - n_1$.*

Abbiamo visto che il sistema minimale di generatori di un semigruppo numerico S è l'insieme $S^* \setminus (S^* + S^*) = M \setminus 2M$, quindi $ed(S) = |M \setminus 2M|$. Dal Corollario 1.3.8 abbiamo che $|M \setminus 2M| = \min M$, cioè $ed(S) = m(S)$ se e solo se M è stabile.

Corollario 1.4.4. *Per un semigruppo numerico S le seguenti affermazioni sono equivalenti*

1. *M è stabile.*
2. *$ed(S) = m(S)$.*

1.5 Semigruppi numerici di Arf

In questa sezione presentiamo una particolare classe di semigruppi numerici di dimensione d'immersione massima: i semigruppi numerici di Arf.

Sia $S = \{0 = s_0 < s_1 < s_2 < \ldots < s_i < s_{i+1} < \ldots\}$ un semigruppo numerico. Introduciamo la seguente notazione

$$S(i) = \{s \in S : s \geq s_i\}.$$

È facile verificare che $S(i)$ è un ideale di S per ogni $i \in \mathbb{N}$.

Definizione 1.5.1. *Diremo che un ideale I di un semigruppo numerico S è **integralmente chiuso** se $I = S(i)$ per qualche $i \in \mathbb{N}$.*

Ad esempio, l'ideale massimale è sempre integralmente chiuso in quanto $M = S(1)$.

Diamo adesso due definizioni equivalenti di semigruppo numerico di Arf: una algebrica (1) e una numerica (2).

Proposizione-Definizione 1.5.2. [6, Theorem 2.2] *Un semigruppo numerico S è di **Arf** se soddisfa una delle seguenti condizioni equivalenti*

1. *Ogni ideale di S integralmente chiuso è stabile.*
2. *Per ogni $x, y, z \in S$ con $x \geq y \geq z$ si ha $x + y - z \in S$.*

Dimostrazione.

$\Rightarrow$ Siano $x, y, z \in S$ con $x \geq y \geq z$ e consideriamo l'ideale integralmente chiuso

$$I = \{s \in S : s \geq z\}.$$

Per ipotesi I è stabile, quindi $2I = I + z$. Osserviamo che $x \geq y \geq z \Rightarrow x, y \in I$, da cui

$$x + y \in 2I = I + z \Rightarrow x + y - z \in I \subseteq S.$$

$\Leftarrow$ Sia I un ideale integralmente chiuso di S. In base al Corollario 1.3.8, ponendo $z = \min I$, ci basta provare che $I - z$ è un semigruppo numerico. Siano $x - z, y - z \in I - z$, dove $x, y \in I$ con $x \geq y \geq z$, allora

$$(x - z) + (y - z) = (x + y - z) - z \in I - z,$$

in quanto $x + y - z \in S$ e $x + y - z \geq z$. Inoltre

$$z + S \subseteq I \Rightarrow S \subseteq I - z \Rightarrow \mathbb{N} \setminus (I - z) \subseteq \mathbb{N} \setminus S,$$

ciò prova che $I - z$ è un semigruppo numerico. □

Dalla definizione algebrica e dalle osservazioni fatte in precedenza segue subito che ogni semigruppo di Arf è di dimensione d'immersione massima. Infatti l'ideale massimale di un semigruppo di Arf è stabile in quanto è integralmente chiuso.

Osservazione 1.5.3. Si noti che se $n = n(S)$ allora tutti gli ideali del tipo $S(i)$ con $i \geq n$ sono stabili in quanto $S(i) - S(i) = \mathbb{N}$. Per cui un semigruppo numerico S è di Arf se e solo se $S(i)$ è stabile per ogni $0 \leq i \leq n$.

Similmente a quanto fatto in [2] studiamo adesso le seguenti tre catene ascendenti di semigruppi numerici.

Sia $S = \{0 = s_0, s_1, \ldots, s_{n-1}, s_n, \rightarrow\}$ un semigruppo numerico (si noti che $n = n(S)$). Definiamo per ogni $i \in \mathbb{N}$

$$S_i = S - S(i) = S(i) - S(i).$$

Per ogni $i \in \mathbb{N}$ abbiamo $S_i \subseteq S_{i+1}$. Infatti sia $x \in S_i$ e $y \in S(i+1) \subseteq S(i)$, allora $x+y \in S(i) \subseteq S$ e $x + y \geq y \geq s_{i+1}$, da cui $x + y \in S(i+1)$, cioè $x \in S_{i+1}$.

Indichiamo con $L(S) = L(S, M)$ il semigruppo di Lipman di S rispetto al suo ideale massimale M. L'operazione $L(S)$ è chiamata anche **blow-up** di S. Definiamo

$$\begin{aligned} L_0 &= S \\ L_{i+1} &= L(L_i) \quad \forall i \in \mathbb{N}. \end{aligned}$$

Osserviamo che $S \subseteq L(S)$ (Proposizione 1.3.4, punto 2), quindi $L_i \subseteq L_{i+1}$.

Indichiamo con $B(S) = M - M = S_1$, dove M è l'ideale massimale di S. Definiamo

$$\begin{aligned} B_0 &= S \\ B_{i+1} &= B(B_i) \quad \forall i \in \mathbb{N}. \end{aligned}$$

Di nuovo dal fatto che $S \subseteq B(S)$ (Proposizione 1.3.4, punto 2), segue che $B_i \subseteq B_{i+1}$.

Dunque per un semigruppo numerico S possiamo considerare le tre catene ascendenti di semigruppi numerici

$$\begin{aligned} S = S_0 \subseteq S_1 \subseteq \ldots \subseteq S_i \subseteq \ldots \subseteq \mathbb{N} \\ S = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_i \subseteq \ldots \subseteq \mathbb{N} \\ S = B_0 \subseteq B_1 \subseteq \ldots \subseteq B_i \subseteq \ldots \subseteq \mathbb{N}. \end{aligned}$$

Osserviamo che esse devono necessariamente essere finite in quanto $\mathbb{N} \setminus S$ è finito. Dall'Osservazione 1.5.3 si ha $S_n = S_{n+1} = \ldots = \mathbb{N}$, quindi la prima catena si stabilizza su $\mathbb{N}$. Inoltre

$S = S_1$ se e solo se $n = 0$, cioè $S = \mathbb{N}$. Osserviamo infine che $B_1 = M - M = S(1) - S(1) = S_1$ e che $S \subseteq M - M \subseteq L(S) \subseteq \mathbb{N}$. Da cui segue

$$S = L(S) \Leftrightarrow S = B(S) \Leftrightarrow S = \mathbb{N}.$$

Teorema 1.5.4. [2, Theorem 1.3.4] *Per un semigruppo numerico S sono equivalenti:*

1. *S è di Arf.*
2. *S_i è stabile per ogni $0 \leq i \leq n(S)$.*
3. *$S_i = S(i) - s_i$.*
4. *Le catene S_i, L_i e B_i coincidono.*
5. *$ed(L_i) = m(L_i)$.*

Dimostrazione.

- (1) $\Leftrightarrow$ (2) Segue dall'Osservazione 1.5.3.
- (2) $\Leftrightarrow$ (3) Di nuovo in base all'Osservazione 1.5.3 è sufficiente dimostrare l'asserto per $0 \leq i \leq n(S)$. Dato che $s_i = \min(S(i))$ dal Corollario 1.3.8 abbimo che $S_i = S(i) - S(i)$ è stabile se e solo se $S_i = S(i) - s_i$.
- (3) $\Leftrightarrow$ (4) $\Leftrightarrow$ (5) Proviamo l'equivalenza per induzione su i. Per $i = 1$ dal Corollario 1.3.8 abbiamo
$$S_1 = M - s_1 \Leftrightarrow S_1 = B_1 = L_1 \Leftrightarrow ed(L_0) = m(L_0).$$
Adesso supponiamo che per $j < i$ si abbia
$$S_j = S(j) - s_j \Leftrightarrow S_j = B_j = L_j \Leftrightarrow ed(L_{j-1}) = m(L_{j-1}).$$
Poniamo $T = S_{i-1}$. Per ipotesi $T = S_{i-1} = B_{i-1} = L_{i-1} = S(i-1) - s_{i-1}$. Allora $T(1) = S(i) - s_{i-1}$ ha $s_i - s_{i-1}$ come elemento minimo e
$$T_1 = T - T(1) = (S(i-1) - s_{i-1}) - (S(i) - s_{i-1}) = S(i-1) - S(i) = S - S(i) = S_i.$$
In base al Corollario 1.3.8 si ha che
$$T_1 = T(1) - (s_i - s_{i-1}) \Leftrightarrow T_1 = B(T) = L(T) \Leftrightarrow ed(T) = m(T)$$
Dato che $B(T) = B_i$, $L(T) = L_i$ e $T(1) - (s_i - s_{i-1}) = S(i) - s_i$ riscrivendo la precedente equazione otteniamo
$$S_i = S(i) - s_i \Leftrightarrow S_i = B_i = L_i \Leftrightarrow ed(L_{i-1}) = m(L_{i-1}).$$ □

Osservazione 1.5.5. Dal punto 5 del teorema precedente segue facilmente che anche il blow-up di un semigruppo numerico di Arf è di Arf.

Dalla definizione numerica di semigruppo numerico di Arf otteniamo il seguente risultato.

Proposizione 1.5.6. [8, Proposition 1] *L'intersezione di due semigruppi numerici di Arf è un semigruppo numerico di Arf.*

In questo modo, se S è un semigruppo numerico, dato che $\mathbb{N}\setminus S$ è finito, i semigruppi numerici di Arf contenenti S sono in numero finito, quindi la loro intersezione è un semigruppo numerico di Arf.

Definizione 1.5.7. *Sia $A \subseteq \mathbb{N}$ con $MCD(A) = 1$, si definisce semigruppo numerico di Arf generato da A, e si indica con $\mathrm{Arf}(A)$, l'intersezione di tutti i semigruppi numerici di Arf contenenti A (e quindi $\langle A \rangle$).*
*Se S è un semigruppo numerico allora $\mathrm{Arf}(S)$ è detta **chiusura di Arf** di S.*

Lemma 1.5.8. [8, Lemma 14] *Se S è un semigruppo numerico di Arf e $x \in S$ allora $\{0\}\cup(x+S)$ è un semigruppo numerico di Arf.*

Dimostrazione. È immediato verificare che $\{0\} \cup (x + S)$ è un semigruppo numerico. Siano $x + s_1, x + s_2, x + s_3 \in x + S$ con $x + s_1 \geq x + s_2 \geq x + s_3$, quindi $s_1 \geq s_2 \geq s_3$. Poiché S è di Arf allora $s_1 + s_2 - s_3 \in S$, cioè $(x + s_1) + (x + s_2) - (x + s_3) = x + (s_1 + s_2 - s_3) \in x + S$. □

Lemma 1.5.9. *Sia S un semigruppo numerico. Risulta $m(S) = m(\mathrm{Arf}(S))$.*

Dimostrazione. È sufficiente osservare che $\{0\} \cup (m(S) + \mathbb{N})$ è un semigruppo di Arf (lemma precedente) contenente S. □

Definizione 1.5.10. *Sia S un semigruppo numerico. Come prima consideriamo la successione L_i dei blow-up di S. Si definisce **successione di molteplicità** di S la successione*

$$(e_0, e_1, e_2, \ldots) \quad \text{con } e_i = m(L_i).$$

Osservazione 1.5.11. Per quanto osservato prima sappiamo che per j sufficientemente grande $L_j = L_{j+1} = \mathbb{N}$, quindi anche $e_j = e_{j+1} = 1$.

Proposizione 1.5.12. *Sia S un semigruppo numerico. Si ha*

$$\mathrm{Arf}(L(S)) = L(\mathrm{Arf}(S)).$$

In altri termini, la chiusura di Arf commuta con il blow-up.

Dimostrazione. Sia N l'ideale massimale di $\mathrm{Arf}(S)$, M l'ideale massimale di S e $r = r(M)$. Adesso dal Lemma 1.5.9 abbiamo che $m(\mathrm{Arf}(S)) = m(S) = m$. Per il Corollario 1.3.8 applicato a rM segue che $L(S) = rM - rM = rM - rm$. Infine, dall'Osservazione 1.5.5 risulta che $L(\mathrm{Arf}(S))$ è di Arf, quindi

$$L(\mathrm{Arf}(S)) = N - N = N - m = rN - rm.$$

Pertanto risulta

$$L(S) = rM - rm \subseteq rN - rm = L(\mathrm{Arf}(S))$$

da cui, essendo $L(\mathrm{Arf}(S))$ un semigruppo numerico di Arf contenente $L(S)$ abbiamo che $\mathrm{Arf}(L(S)) \subseteq L(\mathrm{Arf}(S))$.
Viceversa, sia $V = \{0\} \cup (m + \mathrm{Arf}(L(S)))$. Quest'ultimo è un semigruppo numerico di Arf in base al Lemma 1.5.8. Inoltre V contiene S, infatti si ha

$$M - m \subseteq L(S) \subseteq \mathrm{Arf}(L(S))$$

(dove la prima inclusione segue dalla Proposizione 1.3.6) da cui

$$V = \{0\} \cup (m + \mathrm{Arf}(L(S))) \supseteq \{0\} \cup (m + M - m) = S.$$

Essendo V di Arf abbiamo che $\mathrm{Arf}(S) \subseteq V$. Posto P l'ideale massimale di V e Q l'ideale massimale di $\mathrm{Arf}(S)$, risulta

$$\mathrm{Arf}(S) \subseteq V \Rightarrow Q \subseteq P \Rightarrow L(\mathrm{Arf}(S)) = Q - m \subseteq P - m = L(V) = \mathrm{Arf}(L(S)). \qquad \square$$

Corollario 1.5.13. *I due semigruppi numerici S e $\mathrm{Arf}(S)$ hanno la stessa successione di molteplicità.*

Dimostrazione. Basta osservare che

$$e_i = m(L_i(S)) = m(\mathrm{Arf}(L_i(S))) = m(L_i(\mathrm{Arf}(S)))$$

dove con $L_i(S)$ intendiamo $\underbrace{L(\dots L(L(}_{i \text{ volte}}S)))$. $\square$

Proposizione 1.5.14. *Se $S = \{0 = s_0, s_1, s_2, \dots, s_{n-1}, s_n, \rightarrow\}$ è un semigruppo numerico di Arf, allora $e_i = s_{i+1} - s_i$*

Dimostrazione. Dal Teorema 1.5.4 abbiamo che

$$e_i = m(L_i) = m(S_i) = m(S(i) - s_i) = s_{i+1} - s_i. \qquad \square$$

Dalla proposizione precedente segue che se un semigruppo numerico di Arf S ha successione di molteplicità $(e_0, e_1, \dots, e_{n-1}, e_n, \dots)$ allora

$$S = \{0, e_0, e_0 + e_1, e_0 + e_1 + e_2, \dots\},$$

o in modo equivalente

$$s_k = e_0 + e_1 + \dots + e_{k-1} = \sum_{i=0}^{k-1} e_i.$$

In questo modo, in base a quanto dimostrato finora segue che ogni successione di molteplicità di qualche semigruppo numerico S è associata ad un unico semigruppo numerico di Arf (che non è altro che $\mathrm{Arf}(S)$) ed essa lo determina completamente.
A questo punto possiamo chiederci quali successioni di numeri naturali sono successioni di molteplicità di qualche semigruppo numerico S.

Definizione 1.5.15. *Una successione $\{e_i\}_{i \in \mathbb{N}} \subseteq \mathbb{N}$ è detta **successione di Arf** se è la successione di molteplicità di qualche semigruppo numerico S.*

Proposizione 1.5.16. *Un successione $\{e_i\}_{i \in \mathbb{N}}$ è una successione di Arf se e solo se sono verificate le seguenti condizioni*

1. *Esiste $n \in \mathbb{N}$ tale che per ogni $k \geq n$ si ha $e_k = 1$.*
2. *$e_i = \sum_{j=1}^{h} e_{i+j}$ per qualche $h \in \mathbb{N}$.*

Dimostrazione.

$\Rightarrow$ 1. Supponiamo che $\{e_i\}_{i \in \mathbb{N}}$ sia la successione di Arf associata al semigruppo numerico di Arf $S = \{s_0, s_1, \dots, s_{n-1}, s_n, \rightarrow\}$. Essendo s_n il conduttore di S si ha $s_{k+1} = s_k + 1$ per ogni $k \geq n$, pertanto

$$\forall k \geq n \quad e_k = s_{k+1} - s_k = s_k + 1 - s_k = 1.$$

2. Sia $i \in \mathbb{N}$. Dato che S è di Arf abbiamo che $2s_{i+1} - s_i = s_{i+h+1} \in S$ per qualche $h \in \mathbb{N}$, in quanto $2s_{i+1} - s_i \geq s_{i+1}$. Pertanto

$$e_i = s_{i+1} - s_i = s_{i+h+1} - s_{i+1} = \sum_{j=0}^{i+h} e_j - \sum_{j=0}^{i} e_j = \sum_{j=i+1}^{i+h} e_j = \sum_{j=1}^{h} e_{i+j}$$

$\Leftarrow$ Basta dimostrare che l'insieme

$$S = \{0, e_0, e_0 + e_1, e_0 + e_1 + e_2, \ldots\}$$

è un semigruppo numerico di Arf. Per fare ciò poniamo

$$\begin{aligned} &S_0 = \mathbb{N}, \\ &S_i = \{0\} \cup (e_{n-i} + S_{i-1}) \quad i \geq 1; \end{aligned}$$

in base al Lemma 1.5.8 abbiamo che ogni S_i è un semigruppo numerico di Arf per ogni $i \in \{0, 1, \ldots, n\}$. Infine osserviamo che $S = S_n$. □

Osservazione 1.5.17. Dalla seconda condizione della proposizione precedente segue che se $(e_0, e_1, e_2, \ldots)$ è una successione di Arf, allora $e_i \geq e_{i+1}$ per ogni $i \in \mathbb{N}$.

Capitolo 2

Duplicazione numerica e proprietà di Arf

In questo capitolo presentiamo una costruzione introdotta in [5] e vediamo in che modo essa è legata alla proprietà di Arf.

2.1 Duplicazione numerica

Dato un sottoinsieme $A \subseteq \mathbb{Z}$ e $d \in \mathbb{Z}$ utilizziamo la seguente notazione

$$d \cdot A = \{da : a \in A\}.$$

Per un ideale relativo I di un semigruppo numerico S definiamo $m(I) = \min(I)$, $F(I) = \max(\mathbb{Z} \setminus I)$ e $g(I) = |(\mathbb{Z} \setminus I) \cap (m(I) + \mathbb{N})|$. In particolare se $g(I) > 0$ diremo che l'ideale I ha buchi.

Definizione 2.1.1. *Dato un semigruppo numerico S, un suo ideale I e un elemento dispari $b \in S$, si chiama* ***duplicazione numerica*** *di S rispetto a I e $b \in S$ il seguente sottoinsieme di $\mathbb{N}$*

$$S \bowtie^b I = 2 \cdot S \cup (2 \cdot I + b).$$

È facile verificare che $S \bowtie^b I$ è un semigruppo numerico. Infatti $0 = 2 \cdot 0 \in S \bowtie^b I$ e dato che $F(I) \geq F(S)$, ogni intero $n > 2F(I) + b$ appartiene a $S \bowtie^b I$. Infine il fatto che $b \in S$ e che I è un ideale di S implica che $S \bowtie^b I$ è chiuso rispetto alla somma.

Dalla definizione segue che se $S = \langle n_1, \ldots, n_e \rangle$ e $I = (i_1, \ldots, i_k) + S$ allora

$$S \bowtie^b I = \langle 2n_1, \ldots, 2n_e, 2i_1 + b, \ldots, 2i_k + b \rangle.$$

Osserviamo inoltre che, dato un semigruppo numerico S e $d \in \mathbb{N} \setminus \{0\}$, definendo il **quoziente** ([7], pag. 77)

$$\frac{S}{d} = \{x \in \mathbb{N} : dx \in S\},$$

in generale abbiamo $S = (S \bowtie^b I)/2$.

Analogamente a quanto fatto in [5] diamo la seguente

Definizione 2.1.2. *Un ideale relativo E di un semigruppo numerico S è* ***canonico*** *se risulta $E-(E-I)=I$ per ogni ideale relativo I di S.*
In particolare l'ideale relativo $K(S)=\{x\in\mathbb{Z} : F(S)-x\notin S\}\subseteq\mathbb{N}$ è un ideale canonico che chiameremo ***ideale canonico standard****.*

Tra gli ideali relativi di un semigruppo numerico S possiamo definire la seguente relazione di equivalenza: $E\sim F \Leftrightarrow F=E+x$ per qualche $x\in\mathbb{Z}$. In ogni classe di equivalenza di un ideale relativo E di S esiste un rappresentante $\tilde{E}=E+x$ tale che $F(\tilde{E})=F(S)$.
Osserviamo che gli ideali canonici formano una classe di equivalenza rispetto a questa relazione. Si noti infine che $F(K(S))=F(S)$.

Lemma 2.1.3. [5, Lemma 1.2] *Per un ideale relativo E di un semigruppo numerico S si ha $\tilde{E}\subseteq K(S)\subseteq\mathbb{N}$.*

Dimostrazione. Se per assurdo esistesse $x\in\tilde{E}\setminus K(S)$, allora $F(S)-x\in S$ e pertanto si avrebbe $(F(S)-x)+x=F(S)\in\tilde{E}$, assurdo. □

Lemma 2.1.4. [5, Lemma 1.3] *Sia E un ideale relativo di un semigruppo numerico S. Si ha*

$$n(S)\leq g(\tilde{E})+m(\tilde{E})=|\mathbb{N}\setminus\tilde{E}|,$$

e si ha l'uguaglianza se e solo se E è un ideale canonico di S (cioè $\tilde{E}=K(S)$).

Dimostrazione. È sufficiente osservare che $s\in S\Rightarrow F(S)-s\notin K(S)\supseteq\tilde{E}$. La tesi segue dal fatto che $K(S)\cup(F(S)-S)=\mathbb{Z}$. □

Proposizione 2.1.5. [5, Proposition 2.1] *Siano S un semigruppo numerico, I un suo ideale e $b\in S$ un elemento dispari. Si ha*

1. *$F(S\bowtie^b I)=2F(I)+b$.*
2. *$g(S\bowtie^b I)=g(S)+g(I)+m(I)+\frac{b-1}{2}$.*
3. *$S\bowtie^b I$ è simmetrico se e solo se I è un ideale canonico di S.*

Dimostrazione.

1. Segue da $F(I)\geq F(S)$.
2. I buchi pari di $S\bowtie^b I$ sono in corrispondenza biunivoca con i buchi di S. Tutti gli elemnti dispari minori di $2m(I)+b$ non stanno in $S\bowtie^b I$; infine i buchi dispari maggiori o uguali a $2m(I)+b$ sono in corrispondenza biunivoca con i buchi di I maggiori di $m(I)$.
3. In base alla Proposizione 1.2.4 abbiamo che $S\bowtie^b I$ è simmetrico se e solo se risulta $F(S\bowtie^b I)+1=2g(S\bowtie^b I)$. Usando i punti precedenti otteniamo che $S\bowtie^b I$ è simmetrico se e solo se

$$2F(I)+b+1=2g(S)+2g(I)+2m(I)+b-1\Leftrightarrow$$
$$\Leftrightarrow F(I)+1=g(S)+g(I)+m(I).$$

Dato che abbiamo $m(I)=m(\tilde{I})+(F(S)-F(I))$ e $g(I)=g(\tilde{I})$ sostituendo otteniamo

$$F(I)+1=g(S)+g(\tilde{I})+m(\tilde{I})-F(S)+F(I)\Leftrightarrow$$
$$\Leftrightarrow n(S)=F(S)+1-g(S)=g(\tilde{I})+m(\tilde{I}).$$

Pertanto dal lemma precedente si ha la tesi. □

2.2 La proprietà di Arf nella duplicazione numerica

Facciamo adesso alcune considerazioni sulla proprietà di Arf nel caso della duplicazione numerica.

Una prima semplice osservazione è che, come mostrato nella Proposizione 2.1.5, la proprietà di simmetria della duplicazione numerica non dipende dalla scelta dell'elemento $b \in S$. Ciò non avviene con la proprietà di Arf, come mostra il seguente esempio.

Esempio 2.2.1. Sia $S = \langle 3, 7, 8 \rangle$. La duplicazione numerica si S rispetto al suo ideale massimale M e $b = 3 \in S$ è

$$S \bowtie^3 M = \langle 6, 9, 14, 16, 21, 23 \rangle,$$

che è un semigruppo numerico di Arf, mentre se poniamo $b = 7 \in S$ abbiamo

$$S \bowtie^7 M = \langle 6, 13, 14, 16, 21, 23 \rangle,$$

che non è un semigruppo numerico di Arf, infatti $14 + 14 - 13 = 15 \notin S \bowtie^7 M$.

Proposizione 2.2.2. *Sia S un semigruppo numerico e $d \in \mathbb{N} \setminus \{0\}$. Se S è di Arf allora lo è anche $\frac{S}{d}$.*

Dimostrazione. Supponiamo per assurdo che $\frac{S}{d}$ non sia di Arf, allora devono esistere $x, y, z \in \frac{S}{d}$ tali che $x \geq y \geq z$ e $x + y - z \notin \frac{S}{d}$. Dunque abbiamo $dx, dy, dz \in d \cdot \frac{S}{d} \subseteq S$ con $dx \geq dy \geq dz$ e $dx + dy - dz = d(x + y - z) \notin d \cdot \frac{S}{d}$, quindi necessariamente $d(x + y - z) \notin S$ (altrimenti $(x + y - z) \in \frac{S}{d}$), assurdo. □

Dato che $(S \bowtie^b I)/2 = S$ abbiamo il seguente corollario.

Corollario 2.2.3. *Sia S un semigruppo numerico, I un suo ideale e $b \in S$ un elemento dispari. Se $S \bowtie^b I$ è di Arf allora lo è anche S.*

In altri termini il precedente corollario ci dice che: condizione necessaria affinché la duplicazione numerica $S \bowtie^b I$ sia di Arf è che S sia di Arf.

Lemma 2.2.4. [8, Lemma 11] *Sia $x \in \mathbb{N}$ e $X \subseteq \mathbb{N}$. Se $\{x, x + 1\} \subseteq X$ allora $x + \mathbb{N} \subseteq \mathrm{Arf}(X)$.*

Dimostrazione. Per induzione su n proviamo che $x + n \in \mathrm{Arf}(X)$. Per $n = 0$ abbiamo $x \in X \subseteq \mathrm{Arf}(X)$. Supponiamo adesso che $x+n \in \mathrm{Arf}(X)$, allora $x+(n+1) = (x+n)+(x+1)-x \in \mathrm{Arf}(X)$ poiché $x + n, x + 1, x \in \mathrm{Arf}(X)$ e $x + n \geq x + 1 \geq x$. □

Proposizione 2.2.5. *Sia S un semigruppo numerico e I un suo ideale con buchi ($g(I) > 0$). Allora $S \bowtie^b I$ non è di Arf per $b \in S$ sufficientemente grande.*

Dimostrazione. Fissiamo ad esempio $b > 2F(S)$. Sia $x \in (\mathbb{Z} \setminus I) \cap (\mathbb{N} + m(I))$ (quindi $x \notin I$ e $x > m(I)$). Si ha che $2m(I) + b, 2m(I) + b + 1 \in S \bowtie^b I$, in quanto $2m(I) + b + 1 \geq b > 2F(S)$ e $2m(I) + b + 1$ è pari, ma $2x + b \notin 2 \cdot I + b$, quindi $2x + b \notin S \bowtie^b I$ essendo $2x + b$ dispari. Inoltre $2x + b \geq 2m(I) + b + 1$, pertanto dal lemma precedente $S \bowtie^b I$ non è di Arf. □

Considerando più in generale la duplicazione numerica di un semigruppo numerico S rispetto a un suo ideale relativo E, l'insieme ottenuto è ancora un semigruppo numerico solo nel caso in cui $b + E + E \subseteq S$. Si noti che questa condizione è soddisfatta se b è sufficientemente grande.

Presentiamo adesso una condizione necessaria e sufficiente affinché la duplicazione numerica sia di Arf. A questo scopo, siano

$$S = \{0 = s_0, s_1, \ldots, s_{n-1}, s_n, \rightarrow\}$$

un semigruppo numerico di Arf e $(e_0, e_1, e_2, \ldots)$ la sua successione di molteplicità. In base a quanto detto nel capitolo precedente abbiamo $e_i = s_{i+1} - s_i$, $e_k = 1$ per $k \geq n$ e $e_k > 1$ per $k < n$, essendo s_n il conduttore di S. Sia infine I un ideale di S e $b \in S$ un intero dispari. Con le stesse notazioni abbiamo la seguente

Proposizione 2.2.6. *La duplicazione numerica $D = S \bowtie^b I$ è di Arf se e solo se una delle seguenti condizioni è soddisfatta*

1. $I = x + \mathbb{N}$ *per qualche* $x \geq s_n$.
2. e_0 *è dispari,* $b = e_0 = e_1 = \ldots = e_{n-1}$ *e l'ideale I è integralmente chiuso.*

Inoltre, nel caso in cui sia soddisfatta la condizione 2 ma non la condizione 1 l'ideale I è della forma $I = e_0 \cdot (i + \mathbb{N}) \cup (ne_0 + \mathbb{N})$ per qualche $i < n$ e la successione di molteplicità di D è

$$(\underbrace{2e_0, 2e_0, \ldots, 2e_0}_{i \text{ volte}}, \underbrace{e_0, e_0, \ldots, e_0}_{2(n-i) \text{ volte}}, \underbrace{2, 2, \ldots, 2}_{\frac{e_0-1}{2} \text{ volte}}, 1, \ldots).$$

Dimostrazione.

⇒ Osserviamo che anche la condizione 1 implica che I è integralmente chiuso e dunque supponiamo per assurdo che I non lo sia. Allora esiste $i \in \mathbb{N}$ tale che $s_i \in I$ e $s_{i+1} \notin I$. Supponiamo che $b \geq 2e_i = 2(s_{i+1} - s_i)$, allora si ha $2s_i + b \geq 2s_{i+1} \geq 2s_i$ e, poiché per ipotesi D è di Arf, si ha

$$2s_i + b + 2s_{i+1} - 2s_i = 2s_{i+1} + b \in D \Rightarrow s_{i+1} \in I$$

che è una contraddizione. Quindi $b < 2e_i$, pertanto abbiamo

$$2s_i + b < 2s_{i+1}$$
$$4s_{i+1} - 2s_i - b = 2s_{i+1} + 2e_i - b \in D,$$

dunque $2s_{i+1} + 2e_i - b \in 2 \cdot I + b$, poiché è un intero dispari, con

$$2s_{i+1} + 2e_i - b > 2s_{i+1} > 2s_i + b$$

da cui risulta che $2s_{i+1} + 2e_i - b$ è maggiore o uguale all'intero dispari immediatamente successivo a $2s_i + b$ in D. Poiché $2s_{i+1} + b \notin D$ allora si ha

$$2s_{i+1} + 2e_i - b > 2s_{i+1} + b \Rightarrow b < e_i \leq e_0 = s_1,$$

contro il fatto che $b \in S \setminus \{0\}$, assurdo. Quindi l'ideale I è integralmente chiuso.

Adesso se $n = 0$ allora $S = \mathbb{N}$ e quindi condizione 1 è soddisfatta. Altrimenti supponiamo $n \geq 1$. Se $s_{n-1} \notin I$ allora la condizione 1 è soddisfatta.
Altrimenti, se $s_{n-1} \in I$ supponiamo che $b \geq 2e_{n-1}$, allora

$$2s_{n-1} + b \geq 2s_n.$$

Otteniamo così $2s_{n-1} + b + 1 = 2s_k$ per qualche $k \in \mathbb{N}$ in quanto $2s_{n-1} + b + 1$ è pari e s_n è il conduttore di S. Posto $x = 2s_{n-1} + b$ abbiamo $x, x + 1 \in D$ ed essendo D di Arf, dal Lemma 2.2.4 abbiamo $x + \mathbb{N} \subseteq D$, quindi anche $x + 2 \in D$, cioè

$$\begin{gathered} 2s_{n-1} + b + 2 \in D \\ \Rightarrow s_{n-1} + 1 \in I \\ \Rightarrow s_{n-1} + 1 = s_n \Rightarrow e_{n-1} = 1, \end{gathered}$$

contraddicendo le ipotesi ($e_{n-1} > 1$). Pertanto $b < 2e_{n-1}$, da cui segue

$$\begin{gathered} 2s_{n-1} + b < 2s_n \\ \Rightarrow 2s_n + 2s_n - (2s_{n-1} + b) = 2s_n + 2e_{n-1} - b \in D. \end{gathered}$$

L'ultimo termine è dispari, quindi $2s_n + 2e_{n-1} - b \in 2 \cdot I + b$. Inoltre

$$2s_n + 2e_{n-1} - b \geq 2s_n > 2s_{n-1} + b.$$

Da cui segue che $2s_n + 2e_{n-1} - b$ è maggiore o uguale all'intero dispari immediatamente successivo a $2s_{n-1} + b$ in D, ovvero

$$2s_n + 2e_{n-1} - b \geq 2s_n + b \Rightarrow b \leq e_{n-1} \leq e_0.$$

Dal momento che $b \in S$ ed è dispari ($b \neq 0$) deve aversi

$$b = e_0 = e_1 = \ldots = e_{n-1}.$$

Inoltre l'ideale I è integralmente chiuso, quindi la condizione 2 è soddisfatta.

$\Leftarrow$ Se è soddisfatta la condizione 1 allora $D = 2 \cdot S \cup ((2x + b) + \mathbb{N})$ ed è facile verificare che D è di Arf.
Altrimenti se è soddisfatta la condizione 2 allora $S = e_0 \cdot \mathbb{N} \cup (ne_0 + \mathbb{N})$. In aggiunta possiamo supporre che $n \geq 1$ e che $s_{n-1} \in I$, altrimenti la condizione 1 è soddisfatta, riconducendoci al caso precedente. Pertanto $I = e_0 \cdot (i + \mathbb{N}) \cup (ne_0 + \mathbb{N})$ per qualche $i < n$. Da cui risulta

$$\begin{gathered} D = 2 \cdot S \cup (2 \cdot I + e_0) = \\ = 2e_0 \cdot \mathbb{N} \cup 2 \cdot (ne_0 + \mathbb{N}) \cup e_0 \cdot (2 \cdot (i + \mathbb{N}) + 1) \cup e_0(2n + 1) + \mathbb{N} = \\ = \{0, 2e_0, 4e_0, \ldots, 2ie_0\} \cup \{(2i + 1)e_0, (2i + 2)e_0, (2i + 3)e_0, \ldots (2n - 1)e_0, 2ne_0\} \cup \\ \cup \{2ne_0 + 2, 2ne_0 + 4, \ldots, (2n + 1)e_0 - 3, (2n + 1)e_0 - 1\} \cup ((2n + 1)e_0 + \mathbb{N}). \end{gathered}$$

Ne consegue che se $D = \{0 = d_0 < d_1 < \ldots < d_k < \ldots\}$ allora

$$(d_{k+1} - d_k : k \in \mathbb{N}) = (\underbrace{2e_0, 2e_0, \ldots, 2e_0}_{i \text{ volte}}, \underbrace{e_0, e_0, \ldots, e_0}_{2(n-i) \text{ volte}}, \underbrace{2, 2, \ldots, 2}_{\frac{e_0-1}{2} \text{ volte}}, 1, \ldots).$$

Poiché la successione

$$(\underbrace{2e_0, 2e_0, \ldots, 2e_0}_{i \text{ volte}}, \underbrace{e_0, e_0, \ldots, e_0}_{2(n-i) \text{ volte}}, \underbrace{2, 2, \ldots, 2}_{\frac{e_0-1}{2} \text{ volte}}, 1, \ldots)$$

è una successione di Arf (Proposizione 1.5.16) allora D è di Arf. $\square$

Bibliografia

[1] C. Arf. *Une interpretation algébrique de la suite des ordres de multiplicité d'une branche algébrique.* Proceedings of the London Mathematical Society, 2(1):256–287, 1948.

[2] V. Barucci, D. Dobbs, and M. Fontana. Maximality Properties in Numerical Semigroups and Applications to One-Dimensional Analytically Irreducible Local Domains. Number 598 in American Mathematical Society: Memoirs of the American Mathematical Society. American Mathematical Society, 1997.

[3] M. Bras-Amorós. *Fibonacci-like behavior of the number of numerical semigroups of a given genus.* In Semigroup Forum, volume 76, pages 379–384. Springer, 2008.

[4] F. Curtis. *On formulas for the Frobenius number of a numerical semigroup.* Mathematica Scandinavica, pages 190–192, 1990.

[5] M. D'Anna and F. Strazzanti. *The numerical duplication of a numerical semigroup.* In Semigroup forum, volume 87, pages 149–160. Springer, 2013.

[6] J. Lipman. *Stable ideals and Arf rings.* American Journal of Mathematics, 93(3):649–685, 1971.

[7] J. C. Rosales and P. A. García-Sánchez. Numerical semigroups, volume 20. Springer Science & Business Media, 2009.

[8] J. C. Rosales, P. A. Garcıa-Sánchez, J. I. Garcıa-Garcıa, and M. B. Branco. *Arf numerical semigroups.* Journal of Algebra, 276(1):3–12, 2004.

[9] J. J. Sylvester et al. *Mathematical questions with their solutions.* Educational times, 41(21):6, 1884.

[10] O. Zariski. *Studies in Equisingularity I Equivalent Singularities of Plane Algebroid Curves.* American Journal of Mathematics, 87(2):507–536, 1965.