LE MATEMATICHE
Vol. LXIV (2009) – Fasc. I, pp. 127–145

CORPIDI E LORO PROPRIETÀ

MARIA SCAFATI TALLINI - MAURIZIO IURLO

A corpid is a ring $(K,+,\cdot)$, different from zero, such that $(K,\cdot)$ is an inverse semigroup. We prove a characterization of corpids, some remarkable results about the lattice of the idempotents and other results concerning the idempotents and the zero divisors of a corpid. Finally, we are studiyng a notable set of ideals of corpids through which we study the endomorfisms of a corpid.

Sommario

Si fornisce una caratterizzazione dei corpidi, dimostrando che ogni corpide con un numero finito di idempotenti è isomorfo al prodotto diretto di un numero finito di campi. In particolare, ogni corpide finito è commutativo e isomorfo a un numero finito di campi di Galois. Inoltre si studia il reticolo degli idempotenti di un corpide e si danno proprietà degli idempotenti e dei divisori dello zero di un corpide. Si considera, inoltre, una famiglia notevole di ideali di un corpide, per mezzo della quale si studiano gli endomorfismi di un corpide.

1. Definizioni e richiami

Un corpide K è un anello, non ridotto al solo 0, tale che il semigruppo moltiplicativo $(K,\cdot)$ sia un semigruppo inverso.

Entrato in redazione: 10 febbraio 2009

AMS 2000 Subject Classification: 16E50
Keywords: ring, inverse semigroup

In ogni corpide la relazione $\leq$, definita ponendo $a \leq b \Longleftrightarrow ab^{-1}a = a$ è una relazione di equivalenza.

Un elemento non nullo α di K si dice *semplice* se

$$x \in K,\ x \leq \alpha \Longrightarrow [x = 0,\ \text{ oppure }\ x = \alpha].$$

Con $\mathscr{U}$ si indica l'insieme degli elementi idempotenti di K.

Se K è un corpide unitario e u è la sua identità, è noto che ogni elemento $a \in K - \mathscr{U}$ non è in relazione con $\mathscr{U}$. Inoltre, se $\mathscr{U}$ è semplice, allora K è un corpo e viceversa (Teorema 3.1 di [3]).

Con Θ si indica l'insieme degli elementi semplici (e quindi non nulli) di K. Quando Θ è non vuoto, per ogni $\theta_i, \theta_j \in \Theta$, si ha (cfr (27) in [3])

$$\theta_i \neq \theta_j \Longrightarrow \theta_i \cdot \theta_j = 0.$$

I corpidi con un numero finito di elementi idempotenti (e quindi i corpidi finiti) sono tali che l'insieme Θ è non vuoto (Teorema 3.4 di [3]).

Ogni corpide è privo di elementi nilpotenti (Teorema 3.7 di [3]).

2. Una caratterizzazione dei corpidi

Nel quarto paragrafo dell'articolo [3], sono state poste le seguenti tre ipotesi:

i) $\Theta \neq \emptyset$;

ii) $\forall \alpha \in K, \forall \theta \in \Theta$ si ha $a\theta = \theta a$;

iii) $\forall e \in \mathscr{U} - \{0\}, \exists \theta \in \Theta$ tale che $\theta \leq e$

e si è dimostrato che ogni corpide che soddisfa alle tre condizioni è isomorfo a un sottocorpide $\overline{K}$ di un prodotto diretto di corpi $\{K_i\}_{i \in \mathscr{I}}$ tale che $\overline{K} \supset \oplus_{i \in \mathscr{I}} K_i$ (Teorema 4.1 di [3]). Inoltre, come corollari, si sono dedotti i due seguenti risultati:

- Un corpide K, con Θ non vuoto, soddisfacente alle *ii) e iii)* è isomorfo alla somma diretta di un numero finito di corpi.
- Un corpide K con $\mathscr{U}$ finito e quindi Θ finito, soddisfacente alla *ii),* è somma diretta di un numero finito di corpi. In particolare, se K è commutativo e $\mathscr{U}$ è finito, K è isomorfo a una somma diretta di campi, dunque ogni corpide finito commutativo è somma diretta di campi di Galois in numero finito.

Adesso si dimostrerà la validità della condizione *ii)* in ogni corpide K, in cui l'insieme Θ degli elementi idempotenti è non vuoto. Quindi si dedurrà che ogni corpide K, con $\mathscr{U}$ finito, è isomorfo al prodotto diretto di un numero finito di corpi e, in particolare, ogni corpide finito è commutativo e isomorfo a un numero finito di campi di Galois.

Poniamo

$$K_\theta = \{\alpha\theta,\ \ \alpha \in K\}, \qquad \theta \in \Theta. \tag{1}$$

Si ha:

$$a \in K_\theta \Longleftrightarrow a = a\theta. \tag{2}$$

Infatti: $[\Longleftarrow]$

$$a = a\theta \Longrightarrow a \in K_\theta;$$

$[\Longrightarrow]$

$$a \in K_\theta \Longrightarrow a = \alpha\theta,\ \alpha \in K \Longrightarrow a\theta = \alpha\theta^2 = \alpha\theta = a.$$

Dalla (2) si ha:

$$K_\theta = \{a\theta : a = a\theta\}.$$

Inoltre si ha:

$$(a = a\theta,\ a \neq 0) \Longleftrightarrow a^{-1}a = \theta. \tag{3}$$

Infatti: $[\Longleftarrow]$

$$a^{-1}a = \theta \Rightarrow a \neq 0, a = a\theta;$$

$[\Longrightarrow]$

$$\begin{aligned} \big(a \neq 0,\ a^{-1}a = a^{-1}a\theta\big) &\Longrightarrow \big(a \neq 0,\ e = a^{-1}a \in \mathscr{U},\ e = e\theta\big) \\ &\Longrightarrow \big(e \leq \theta,\ e = a^{-1}a \neq 0\big) \\ &\Longrightarrow e = a^{-1}a = \theta \Longrightarrow a^{-1}a = \theta. \end{aligned}$$

Dalla (3) si ottiene

$$K_\theta - \{0\} = \{a \in K : a^{-1}a = \theta\}. \tag{4}$$

K_θ è sottoanello di K e anche un ideale sinistro di K. Proviamo che:

Teorema 2.1. *L'anello K_θ non possiede divisori dello zero.*

Dimostrazione. Ragionando per assurdo, supponiamo che esistano due elementi a, b di K_θ, tali che

$$a \neq 0,\ b \neq 0,\ ab = 0. \tag{5}$$

Per la (4) deve allora aversi (essendo $a, b \in K_\theta - \{0\}$):

$$a^{-1}a = \theta, \quad b^{-1}b = \theta. \tag{6}$$

Per la (6), ricordando che ogni corpide è privo di elementi nilpotenti e che gli elementi bb^{-1}, $b^{-1}b$ commutano perché idempotenti, si ha:

$$\begin{aligned} ab=0 &\implies a^{-1}ab=0 \implies \theta b=0 \implies b^{-1}bb=0 \\ &\implies (bbb^{-1})b^{-1}bb=(bbb^{-1})0=0 \implies b(b^{-1}b)(bb^{-1})b=0 \\ &\implies b^2=0 \implies b=0 \end{aligned}$$

e ciò è escluso, per la (5). L'assurdo prova l'asserto. □

Teorema 2.2. *L'anello K_θ è un corpo che ha come unità θ e tale che l'inverso di ogni elemento $a \in K_\theta$ è dato dall'inverside a^{-1} di a.*

Dimostrazione. L'anello K_θ contiene θ e quindi contiene $a-\theta a$, per ogni $a \in K_\theta$.

Si ha allora dal Teorema 2.1:

$$\begin{aligned} a \in K_\theta - \{0\} &\iff (a=a\theta,\ a\neq 0) \implies a^2=a\theta a \\ &\implies a(a-\theta a)=0 \implies a=\theta a. \end{aligned}$$

Si è cosí provato che:

$$a \in K_\theta \implies a=\theta a. \tag{7}$$

Si ha:

$$\begin{aligned} (a\in K,\ a=\theta a) &\implies a^{-1}=a^{-1}\theta \implies a^{-1}\in K_\theta \\ &\overset{(7)}{\implies} a^{-1}=\theta a^{-1} \implies a=a\theta \\ &\implies a\in K_\theta. \end{aligned}$$

Da ciò e dalla (7), si ricava:

$$a\in K_\theta \iff a=\theta a \iff a=a\theta \iff a=a\theta=\theta a. \tag{8}$$

Dalla (8) si ha che θ è unità di K_θ e inoltre:

$$a\in K_\theta \iff a^{-1}\in K_\theta.$$

Infine, per la (3), si deduce che:

$$\begin{aligned} &a\in K_\theta-\{0\} \implies a^{-1}a=\theta; \\ &\left[(aa^{-1})a=a,\ \theta a=a,\ a\neq 0\right] \implies a^{-1}a=\theta; \\ &\left[(aa^{-1}-\theta)a=0,\ a\neq 0\right] \implies aa^{-1}=\theta,\ a^{-1}a=\theta. \end{aligned}$$

□

Sia α un qualsiasi elemento di K. Per ogni $\theta \in \Theta$, risulta $\alpha\theta \in K_\theta$ (cfr (1)), quindi:

$$(\alpha\theta)^{-1} = \theta\alpha^{-1} \in K_\theta$$

(cfr Teorema 2.2). Ne segue che

$$\begin{aligned}(\alpha\theta)\left(\theta\alpha^{-1}\right) = \left(\theta\alpha^{-1}\right)(\alpha\theta) = \theta \quad &\Longrightarrow \quad \alpha\theta\alpha^{-1} = \theta\left(\alpha^{-1}\alpha\right)\theta = \theta \\ &\Longrightarrow \quad \alpha\theta\alpha^{-1} = \theta = \theta\alpha^{-1}\alpha \\ &\Longrightarrow \quad \left[\alpha\theta = \alpha\theta\alpha^{-1}\alpha,\ \alpha\theta\alpha^{-1} = \theta\right] \\ &\Longrightarrow \quad \alpha\theta = \theta\alpha.\end{aligned}$$

Si è cosí provata la *ii)*, cioè la (33) di [3]. Posto $\Theta = \{\theta_i\}_{i\in\mathscr{I}}$, $\theta_i \neq \theta_j$ per $i \neq j$, e $K_i = K_{\theta_i}$, si consideri l'applicazione:

$$\varphi : \alpha \in K \longmapsto \{\alpha\theta_i\}_{i\in\mathscr{I}} \in \otimes_{i\in\mathscr{I}} K_i.$$

In forza della *ii)*, l'applicazione φ è un omomorfismo. Si ha:

$$\alpha \in \ker\varphi \Longleftrightarrow \alpha\theta_i = \theta_i\alpha = 0, \quad \forall i \in \mathscr{I}.$$

Si prova il seguente:

Teorema 2.3.

$$e \in \mathscr{U}, \quad e \notin \ker\varphi \Longleftrightarrow \textit{e ammette un minorante semplice.} \tag{9}$$

Dimostrazione. Infatti:

$$\begin{aligned}e \notin \ker\varphi \quad &\Longleftrightarrow \quad \exists\tau \in \Theta : e\tau \neq 0 \\ &\Longleftrightarrow \quad \exists\tau \in \Theta : 0 \neq e\tau \leq \tau \\ &\Longleftrightarrow \quad \exists\tau \in \Theta : e\tau = \tau \Longleftrightarrow \exists\tau \in \Theta : \tau \leq e.\end{aligned}$$

□

Pertanto, dal Teorema 2.3 si ricava che:

$$e \in \mathscr{U}, \quad e \in \ker\varphi \Longleftrightarrow e \text{ non ammette un minorante semplice.}$$

Dal Teorema 2.3 si ha anche:

$$\ker\varphi = \{0\} \Longleftrightarrow [\forall e \in \mathscr{U} - \{0\} \quad \exists\tau \in \Theta : \tau \leq e]. \tag{10}$$

Essendo la ϕ un omomorfismo, si ha che $K/\ker\varphi \simeq \operatorname{Im}\varphi$. Ne segue che:

Teorema 2.4. *Sia K un corpide soddisfacente alla (10). Posto $K_i = \{a \in K : \alpha = \alpha\tau_i\}$, K_i è un corpo, K è isomorfo a un sottocorpide del prodotto diretto $\otimes_{i\in\mathscr{I}} K_i$ che contiene la somma diretta $\oplus_{i\in\mathscr{I}} K_i$. In particolare, se Θ è finito, risulta $K \simeq \otimes_{i\in\mathscr{I}} K_i$.*

Osservato che se $\mathscr{U}$ è finito la (10) è verificata, come corollario deduciamo il seguente:

Teorema 2.5. *Ogni corpide K con $\mathscr{U}$ finito è isomorfo al prodotto diretto di un numero finito di corpi. In particolare ogni corpide finito è commutativo e isomorfo a una somma diretta di un numero finito di campi di Galois.*

Ne segue che:

Teorema 2.6. *Ogni corpide con $\mathscr{U}$ finito è unitario.*

3. Reticolo degli idempotenti in un corpide

Sia A un qualsiasi anello con unità u e con idempotenti tra loro permutabili e sia $\mathscr{U}$ l'insieme degli idempotenti di A. L'insieme $\mathscr{U}$ è ovviamente chiuso rispetto al prodotto. Ricordiamo la seguente relazione d'ordine in $\mathscr{U}$ (vedi (7) di [3]):

$$e, \eta \in \mathscr{U}, \quad e \leq \eta \Longleftrightarrow e = e\eta. \tag{11}$$

Sussiste il seguente

Teorema 3.1. *Si ha per ogni $e, \eta \in \mathscr{U}$*

$$e\eta \leq e,\ e\eta \leq \eta, \tag{12}$$

$$\forall \tau \in \mathscr{U} : \tau \leq e, \quad \tau \leq \eta \Longrightarrow \tau \leq e\eta. \tag{13}$$

Dimostrazione.

$$\begin{aligned} (\tau \leq e,\ \tau \leq \eta) &\Longrightarrow (\tau = \tau e,\ \tau = \tau\eta) \Longrightarrow \tau^2 = \tau^2 e\eta \\ &\Longrightarrow \tau = \tau e\eta \Longrightarrow \tau \leq e\eta. \end{aligned}$$

□

Dalle (12) e (13) segue che

$$\forall e, \eta \in \mathscr{U},\ e\eta \text{ è il massimo dei confini inferiori di } \{e, \eta\}. \tag{14}$$

Si ha:

$$\forall e, \eta \in \mathscr{U}, \quad e \leq e + \eta - e\eta,\ \ \eta \leq e + \eta - e\eta. \tag{15}$$

Infatti:

$$e = e(e+\eta-e\eta), \quad \eta = \eta\,(e+\eta-e\eta)\,.$$

Si ha inoltre, per ogni $e,\eta \in \mathscr{U}$:

$$(\forall \tau \in \mathscr{U} : e \le \tau,\ \eta \le \tau) \Longrightarrow e+\eta-e\eta \le \tau. \tag{16}$$

Infatti:

$$\begin{aligned}(e \le \tau,\ \eta \le \tau) &\Longrightarrow (e = e\tau,\ \eta = \eta\tau)\\ &\Longrightarrow e+\eta-e\eta = e\tau+\eta\tau-e\eta\tau = (e+\eta-e\eta)\,\tau\\ &\Longrightarrow e+\eta-e\eta \le \tau.\end{aligned}$$

Dalle (15) e (16) segue che:

$$\forall e,\eta \in \mathscr{U},\ \ e+\eta-e\eta \ \text{ è il minimo dei confini superiori di } \{e,\eta\}\,. \tag{17}$$

Da (14) e (17) si ricava che

Teorema 3.2. *$(\mathscr{U},\le)$ è un reticolo e si ha $e\cap\eta = e\eta$, $e\cup\eta = e+\eta-e\eta$.*

Risulta:

$$e\cap 0 = 0, \quad e\cup 0 = e, \quad u\cap e = e, \quad u\cup e = e, \tag{18}$$

$$\forall e \in \mathscr{U} \ \ \exists e' = u-e : e\cap e' = 0,\ \ e\cup e' = u. \tag{19}$$

Dal Teorema (3.2) e dalle (18) e (19) segue che:

Teorema 3.3. *Sia A un anello unitario i cui idempotenti siano tra loro permutabili (in particolare A sia un corpide). Denotato con $\mathscr{U}$ l'insieme degli idempotenti di A, si ha che $(\mathscr{U},\le)$ è un'algebra di Boole, il cui anello booleano associato è dato da $(\mathscr{U},\oplus,\odot)$, con*

$$e\oplus\eta = e+\eta-e\eta, \qquad e\odot\eta = e\eta.$$

Si ha poi (vedi [2], Esempio 2.2):

Teorema 3.4. *Un corpide in cui ogni elemento è un idempotente è un anello booleano e, viceversa, un anello booleano è un corpide.*

4. Proprietà degli idempotenti e dei divisori dello zero in un corpide

Sia K un corpide unitario e sia $\mathscr{U}$ l'insieme degli idempotenti di K. Sia $e \in \mathscr{U} - \{0\}$. Si consideri l'applicazione

$$\varphi_e : n \in \mathbb{Z} \longmapsto ne \in K.$$

L'applicazione φ è un omomorfismo dell'anello $\mathbb{Z}$ nell'anello K. Infatti:

$$\begin{aligned} &\varphi_e(n+m) = (n+m)e = ne + me = \varphi(n) + \varphi(m), \\ &\varphi_e(nm) = nme = (ne)(me) = \varphi_e(n)\varphi_e(m). \end{aligned}$$

Se e ha periodo q, risulta $\ker \varphi_e = \{qz\}_{z\in\mathbb{Z}}$ e quindi $\operatorname{Im} \varphi_e \simeq \mathbb{Z}_q$. Inoltre, poiché in K non ci sono nilpotenti, q non ammette fattori propri multipli, cioè q è semplice. Infatti, se fosse $q = t^2 p$, sarebbe $tp \neq 0$ e inoltre $(tp)^2 = t^2 p \cdot p = 0$. Allora $\operatorname{Im} \varphi_e \equiv \mathbb{Z}_q$ è un sottocorpide di K e coincide con il sottocorpide di K generato da e.
Se e ha periodo infinito, $\ker \varphi_e = \{0\}$ e, quindi, $\operatorname{Im} \varphi_e \simeq \mathbb{Z}$.

Si ha, se $e, \eta \in \mathscr{U}$,

$$e \leq \eta \Longrightarrow \eta - e \in \mathscr{U}, \quad \eta - e \leq \eta.$$

Infatti, ricordando la (11)

$$\begin{aligned} (\eta - e)^2 &= \eta + e - e\eta - \eta e \\ &= \eta + e\eta - e\eta - e\eta = \eta - e, \end{aligned}$$

$$\eta - e = (\eta - e)\,\eta \Longrightarrow \eta - e \leq \eta.$$

Si ha ancora:

$$e, \eta \in \mathscr{U}, \qquad e \leq \eta \Longrightarrow ne \leq n\eta, \quad \forall n \in \mathbb{Z}.$$

Infatti:

$$e \leq \eta \Longleftrightarrow e = e\eta \Longrightarrow ne = (n\eta)\,e \leq n\eta. \tag{20}$$

Dalla (20) segue il seguente teorema:

Teorema 4.1. *Fissato un idempotente e di un corpide K, se esso ha periodo infinito, allora ogni idempotente che ne sia maggiorante ha periodo infinito. Se l'idempotente e ha periodo q, ogni idempotente minorante l'idempotente e e ha periodo dato da un divisore di q.*

Proviamo che

$$aa^{-1} = a^{-1}a, \qquad \forall a \in K. \tag{21}$$

Poniamo:

$$b = aa^{-1} - a^{-1}a. \tag{22}$$

Si ha:

$$ab = a^2a^{-1} - aa^{-1}a = a^2a^{-1} - a \Longrightarrow aba = a^2 - a^2 = 0$$

e

$$(ba)^2 = (ba)(ba) = b(aba) = 0,$$

da cui

$$ba = 0,$$

altrimenti ba sarebbe nilpotente (cfr [3], Teorema 9). Ma

$$\begin{aligned} [ab = 0,\ ba = 0] \quad &\Longrightarrow \quad \left[a^2a^{-1} = a,\ a = a^{-1}a^2\right] \\ &\Longrightarrow \quad \left[a^{-1}a^2a^{-1} = a^{-1}a,\ aa^{-1} = a^{-1}a^2a^{-1}\right] \\ &\Longrightarrow \quad aa^{-1} = a^{-1}a, \end{aligned}$$

quindi la (21).

Sia $\mathscr{O}_s$ l'insieme costituito dallo zero e dai divisori dello zero sinistri del corpide K, cioè:

$$a \in \mathscr{O}_s \overset{\text{def}}{\Longleftrightarrow} \exists \alpha \in K - \{0\} : a\alpha = 0.$$

Sia $\mathscr{O}_d$ l'insieme costituito dallo zero e dai divisori dello zero destri di K, cioè:

$$a \in \mathscr{O}_d \overset{\text{def}}{\Longleftrightarrow} \exists \beta \in K - \{0\} : \beta b = 0.$$

Proviamo che:

Teorema 4.2. *In un corpide K ogni divisore dello zero sinistro è anche divisore dello zero destro:*

$$a, b \in K - \{0\}, \qquad ab = 0 \Longleftrightarrow ba = 0. \tag{23}$$

Dimostrazione. Si ha:

$$\begin{aligned} ab = 0 \quad &\Longrightarrow \quad b^{-1}a^{-1} = 0 \Longrightarrow b^{-1}a^{-1}a = 0 \overset{(21)}{\Longrightarrow} b^{-1}aa^{-1} = 0 \\ &\Longrightarrow \quad b^{-1}\left(aa^{-1}a\right) = 0 \Longrightarrow b^{-1}a = 0 \Longrightarrow bb^{-1}a = 0 \overset{(21)}{\Longrightarrow} b^{-1}ba = 0 \\ &\Longrightarrow \quad ba = 0, \end{aligned}$$

onde la (23). Dalla (23) segue che ogni divisore dello zero sinistro è anche divisore dello zero destro e viceversa, cioè

$$\mathscr{O}_s = \mathscr{O}_d.$$

□

Ricordando che era stato denominato con $\mathscr{O}$ l'insieme costituito dallo zero e dai divisori dello zero di K, si ha, quindi, per il teorema precedente:

$$\mathscr{O} = \mathscr{O}_s = \mathscr{O}_d.$$

Proviamo inoltre che

Teorema 4.3. *Si ha $K \neq \mathscr{O}$ se, e soltanto se, K è unitario.*

Dimostrazione. [$\Longleftarrow$] Se K è unitario, la sua unità non è un divisore dello zero, onde $K \neq \mathscr{O}$.
[$\Longrightarrow$] Se $K \neq \mathscr{O}$, esiste $a \in K - \mathscr{O}$. Posto $v = aa^{-1}$, risulta $v \notin \mathscr{O}$ (infatti in caso contrario esisterebbe un $b \neq 0$ in K, tale che $bv = 0$, onde $baa^{-1} = 0$, da cui $ba = baa^{-1}a = 0$, e ciò è escluso, essendo $a \in K - \mathscr{O}$). Si ha, per ogni $\alpha \in K$,

$$\alpha v = \alpha v^2, \quad v\alpha = v^2\alpha$$

da cui

$$(\alpha - \alpha v)\, v = 0, \quad v\,(\alpha - \alpha v) = 0,$$

onde (poiché $v \notin \mathscr{O}$)

$$\alpha - \alpha v = 0, \quad \alpha - v\alpha = 0,$$

cioè

$$\alpha = \alpha v = v\alpha,$$

quindi v è l'unità di K, onde la tesi.

□

Dimostriamo il teorema seguente.

Teorema 4.4. *In un corpide K gli idempotenti sono permutabili con tutti gli elementi di K, cioè si ha:*

$$\forall a \in K, \ \forall e \in \mathscr{U}, \qquad ae = ea. \tag{24}$$

Dimostrazione. Infatti:

$$e^2 = e \implies \left(ae^2 = ae,\ e^2a = ea\right) \implies \left(ae^2 - ae = 0,\ e^2a - ea = 0\right)$$

$$\implies ((ae - a)\, e = 0,\ e\,(ea - a) = 0) \overset{(23)}{\Longrightarrow} (e\,(ae - a) = 0,\ (ea - a)\, e = 0)$$

$$\implies (eae - ea = 0,\ eae - ae = 0) \implies eae = ea = ae,$$

onde la (24). □

Sia K un corpide. Si ha:

$$\forall a \in K, \qquad na = 0 \Longleftrightarrow n\left(aa^{-1}\right) = 0, \quad n \in \mathbb{Z}.$$

Ne segue che

Teorema 4.5. *Ogni $a \in K$ ha periodo uguale all'idempotente aa^{-1}.*

5. Studio di una famiglia notevole di ideali di un corpide

Sia K un corpide e sia $\mathscr{U}$ l'insieme dei suoi idempotenti. Per ogni $e \in \mathscr{U}$ si ponga

$$K_e = \{\alpha e\}_{\alpha \in K}.$$

Si ha:

$$a = \alpha e \Longrightarrow ae = \alpha e = a$$

e quindi (cfr (24) e (21)):

$$a \in K_e \Longleftrightarrow a = ae \Longleftrightarrow a^{-1}a \leq e \Longleftrightarrow a = ea \Longleftrightarrow aa^{-1} \leq e, \qquad (25)$$

pertanto si ottiene che:

$$\begin{aligned} K_e &= \{a \in K : a = ae\} = \{a \in K : a = ea\} \\ &= \{a \in K : aa^{-1} \leq e\} = \{a \in K : a^{-1}a \leq e\}. \end{aligned}$$

Teorema 5.1. *K_e è un ideale bilatero del corpide unitario K. L'unità di K_e è l'unità e del corpide unitario K. Gli elementi che ammettono inverso in K_e, cioè i non divisori dello zero in K_e, sono tutti e soli quegli elementi a non nulli per i quali si ha $aa^{-1} = e$. Inoltre se $e \neq u$, dove u è l'unità di K, ogni elemento a di K_e, diverso da zero, è un divisore dello zero in K, cioè*

$$K_e \subseteq \mathscr{O}.$$

Dimostrazione. Per ogni $\alpha \in K$ e $a, b \in K_e$, si ha:

$$a - b \in K_e, \quad \alpha a \in K_e, \quad a\alpha \in K_e, \quad a^{-1} \in K_e.$$

Infatti:

$$\begin{aligned} (a \in K_e,\, b \in K_e) &\Longrightarrow (a = ae,\, b = be) \Longrightarrow a \pm b = (a \pm b)e \\ &\Longrightarrow a \pm b \in K_e; \\ (\alpha \in K,\, a \in K_e) &\Longrightarrow (\alpha \in K,\, a = ae = ea) \Longrightarrow (\alpha a = (\alpha a)e,\, a\alpha = ea\alpha) \\ &\Longrightarrow (a\alpha \in K_e,\, \alpha a \in K_e) \end{aligned}$$

e quindi K_e è un ideale bilatero.
Inoltre e è ovviamente l'unità di K_e. Infatti,

$$\begin{aligned} \alpha e \cdot e &= \alpha e^2 = \alpha e, \qquad \forall \alpha e \in K_e, \\ e\alpha \cdot e &= \alpha ee = \alpha e^2 = \alpha e, \qquad \forall \alpha e \in K_e. \end{aligned}$$

Dimostriamo ora che gli elementi che ammettono inverso in K_e sono tutti e soli gli elementi non nulli per i quali si ha $aa^{-1} = e$. Per la (23), se $aa^{-1} = e$, si ha

anche $a^{-1}a = e$ e viceversa. Inoltre ricordiamo che (cfr [2], Teorema 2.4) in un corpide unitario un elemento ammette inverso (coincidente con l'inverside) se, e soltanto se, esso non è né zero, né un divisore dello zero. Ora, se $a \neq 0$, $a \in K_e$, $e \neq u$, allora $aa^{-1} = e \neq u$, per cui a non è invertibile in K e quindi è un divisore dello zero in K.

□

Risulta poi

$$K_u = K, \qquad K_0 = \{0\},$$

$$K_e \subseteq K_\eta \Longleftrightarrow e \leq \eta, \tag{26}$$

$$K_e \cap K_\eta = K_{e\eta}. \tag{27}$$

Dimostriamo la (26). Si ha:

[$\Longrightarrow$]

$$K_e \subseteq K_\eta \Longrightarrow e \in K_\eta \Longrightarrow e = e\eta \Longrightarrow e \leq \eta;$$

[$\Longleftarrow$]

$$\begin{aligned}(a \in K_e,\ e \leq \eta) &\Longrightarrow (a = ae,\ e = e\eta)\\ &\Longrightarrow a = ae = ae\eta = a\eta \Longrightarrow a \in K_\eta \Longrightarrow K_e \subseteq K_\eta.\end{aligned}$$

Dimostriamo la (27). Dimostriamo che $K_e \cap K_\eta \supseteq K_{e\eta}$. Basta dimostrare che $K_{e\eta} \subseteq K_e$, $K_{e\eta} \subseteq K_\eta$. Dalla (26) si ha che se $e\eta \leq e$ allora $K_{e\eta} \subseteq K_e$. Ma $e\eta = e\eta e$, perché $e\eta = e^2\eta = e\eta e$. Analogamente per K_η. Si ha poi:

$$a \in K_e \cap K_\eta \Longrightarrow a = ae = a\eta \Longrightarrow a = ae\eta \Longrightarrow a \in K_{e\eta},$$

quindi

$$K_e \cap K_\eta \subseteq K_{e\eta}$$

Poiché $K_e \cap K_\eta \supseteq K_{e\eta}$, si ha:

$$K_e \cap K_\eta = K_{e\eta}$$

Si consideri l'applicazione:

$$\phi : e \in \mathscr{U} \longmapsto K_e \in \mathbb{P}K.$$

Essa è iniettiva, per la (26); inoltre, sempre per la (26), essa muta la relazione d'ordine $\leq$, definita in $\mathscr{U}$, nella relazione di inclusione. Poiché $(\mathscr{U}, \leq)$ è un'algebra di Boole, ne segue che $\left(\{K_e\}_{e\in\mathscr{U}}, \subseteq\right)$ è un'algebra di Boole. Si ha inoltre (cfr (3.2)):

$$K_e \cap K_\eta = K_{e\eta}. \tag{28}$$

Analogamente:

$$K_e \cup K_\eta = K_{e+\eta-e\eta}, \tag{29}$$

dove $\cup$ rappresenta l'unione disgiunta. Concludendo, si ottiene il seguente:

Teorema 5.2. *La famiglia di ideali di K data da $\{K_e\}_{e\in\mathscr{U}}$, rispetto alla relazione di inclusione $\subseteq$ di K, risulta un'algebra di Boole, isomorfa a $(\mathscr{U},\leq)$, in cui l'unione disgiunta $\dot\cup$ e l'intersezione $\cap$ sono dati dalle (28) e (29). Vale la formula di Grassmann:*

$$(K_e \dot\cup K_\eta = K_c, \quad K_e \cap K_\eta = K_i) \Longrightarrow e+\eta = i+c.$$

Teorema 5.3. *K_e è un corpo se, e soltanto se, e è semplice in K.*

Dimostrazione. Poiché K_e è un corpide, si ha che K_e è un corpo se, e soltanto se, K_e non ammette divisori dello zero (cfr [2], Teorema 2.3). Occorre dunque provare che K_e non ammette divisori dello zero se e solo se e è semplice in K.
[$\Longrightarrow$] Sia $\theta \in \mathscr{U}$, con $\theta \leq e$. Si ha allora $\theta = \theta e$, onde $\theta \in K_e$ (cfr (25)); inoltre $\theta^2 = \theta e$, da cui segue $\theta(\theta - e) = 0$, onde (poiché K_e non ammette divisori dello zero e $\theta \in K_e$, $\theta - e \in K_e$) risulta $\theta = 0$ oppure $\theta = e$. Ne segue che θ è semplice.
[$\Longleftarrow$] Siano $a,b \in K_e$, con $ab = 0$. Si ha $a = ae$ e quindi $a^{-1}a = a^{-1}ae$, onde $a^{-1}a \leq e$. Poiché e è semplice, risulta $a^{-1}a = 0$ oppure $a^{-1}a = e$. Nel primo caso si ha $a = 0$, nel secondo si ha $0 = ab = a^{-1}ab = eb = b$. Ne segue che $ab = 0$ implica $a = 0$, oppure $b = 0$, cioè K_e non ha divisori dello zero. Si è cosí provata la tesi. □

Sia K un corpide qualsiasi. Per ogni $a \in K$, posto $e = aa^{-1} = a^{-1}a$, si consideri l'applicazione:

$$T_a : x \in K_e \longmapsto ax \in K_e.$$

Teorema 5.4. *L'applicazione T_a è un automorfismo additivo di K_e.*

Dimostrazione. Si ha:

$$x,y \in K_e, \qquad T_a(x+y) = a(x+y) = ax+ay = T_a(x)+T_a(y)$$

e inoltre (avendosi, per $y \in K_e$, $y = ey$):

$$T_a(xy) = axy = axey = axa^{-1}ay = T_a(x)a^{-1}T_a(y),$$

cioè T_a è un omomorfismo additivo, cioè una trasformazione lineare di K_e. Si ha:

$$\begin{aligned} x &\in \ker T_a \Longrightarrow x \in K_e,\ ax = 0 \Longrightarrow x = ex,\ ax = 0, \\ x &= a^{-1}ax,\ ax = 0 \Longrightarrow x = 0, \end{aligned}$$

onde è

$$\ker T_a = \{0\},$$

dunque T_a è iniettivo. Essendo $a^{-1} = a^{-1}aa^{-1} = a^{-1}e$, si ha $a^{-1} \in K_e$, quindi:

$$\forall y \in K_e, \qquad y = ey = a\left(a^{-1}y\right) \Longrightarrow \exists x = a^{-1}y \in K_e : y = ax,$$

cioè $\operatorname{Im} T_a = K_e$. Ne segue che

$$T_a : K_e \longrightarrow K_e$$

è biettivo, cioè è un automorfismo additivo di K_e. □

Risulta:

$$\forall e \in \mathscr{U}, \qquad T_e : x \in K_e \longmapsto ex = x \in K_e,$$

cioè:

$$\forall e \in \mathscr{U}, \qquad T_e \text{ l'applicazione identica in } K_e.$$

Proviamo che

$$\forall a, b \in K, \qquad T_a = T_b \Longrightarrow a = b. \tag{30}$$

Si ha (cfr (26)) per ogni $a, b \in K$:

$$\begin{aligned} T_a = T_b &\Longrightarrow [K_{aa^{-1}} = K_{bb^{-1}};\ \forall x \in K_{aa^{-1}} = K_{bb^{-1}},\ ax = bx] && (31)\\ &\Longrightarrow e = aa^{-1} = bb^{-1}; && (32)\end{aligned}$$

Se

$$x = e \in K_e = K_{aa^{-1}} = K_{bb^{-1}},\ ae = be,$$

allora

$$a = a\left(a^{-1}a\right) = ae = be = b\left(b^{-1}b\right) = b,$$

onde la (30).

Si consideri la famiglia di trasformazioni parziali di K date da $\mathscr{T} = \{T_a\}_{a \in K}$. Essa è propria, per la (30), e inoltre per ogni $a \in K$, T_a è un automorfismo additivo di $K_{aa^{-1}}$.

Per ogni $a, b \in K$, si consideri la trasformazione parziale di K data da $T_a \circ T_b$. Essa risulta:

$$T_a \circ T_b : x \in T_b^{-1}\left(K_{aa^{-1}} \cap K_{bb^{-1}}\right) \longmapsto abx \in T_a\left(K_{aa^{-1}} \cap K_{bb^{-1}}\right). \tag{33}$$

Proviamo che

$$\begin{aligned} T_b^{-1}\left(K_{aa^{-1}} \cap K_{bb^{-1}}\right) &= K_{aa^{-1}bb^{-1}}, && (34)\\ T_a\left(K_{aa^{-1}} \cap K_{bb^{-1}}\right) &= K_{aa^{-1}bb^{-1}}. && (35)\end{aligned}$$

Si ha:

$$\left[\forall t \in K, \qquad t = b^{-1}bt,\ bt = a^{-1}abt\right] \Longleftrightarrow \left[t = b^{-1}bt,\ t = a^{-1}at\right]. \tag{36}$$

$[\Longleftarrow]$ Segue subito dalla (24).
$[\Longrightarrow]$ Per la (24), si ha:

$$t = b^{-1}bt,\ bt = a^{-1}abt \Longrightarrow t = b^{-1}a^{-1}abt = a^{-1}ab^{-1}bt = a^{-1}at,\ t = b^{-1}bt.$$

Dalla (36), si ottiene:

$$\begin{aligned} t \in T_b^{-1}\left(K_{aa^{-1}} \cap K_{bb^{-1}}\right) &\Longleftrightarrow t \in K_{bb^{-1}},\ bt \in K_{aa^{-1}} \\ &\Longleftrightarrow t = b^{-1}bt,\ bt = a^{-1}abt \\ &\Longleftrightarrow t = b^{-1}bt,\ t = a^{-1}at \\ &\Longleftrightarrow t \in K_{aa^{-1}} \cap K_{bb^{-1}}, \end{aligned}$$

cioè la (34) (in forza delle (28) e (21)). Inoltre si ha (cfr (24)):

$$\begin{aligned} x \in K_{a^{-1}a} \cap K_{b^{-1}b} &\Longrightarrow \left[x = a^{-1}ax,\ x = b^{-1}bx\right] \\ &\Longrightarrow \left[x = a^{-1}a\left(ax\right),\ ax = b^{-1}b\left(ax\right)\right] \\ &\Longrightarrow ax \in K_{a^{-1}a} \cap K_{b^{-1}b}, \end{aligned}$$

cioè:

$$K_{a^{-1}a} \cap K_{b^{-1}b} \subseteq T_a\left(K_{a^{-1}a} \cap K_{b^{-1}b}\right). \tag{37}$$

D'altra parte si ha (cfr (24)):

$$\begin{aligned} x \in T_a\left(K_{a^{-1}a} \cap K_{b^{-1}b}\right) &\Longrightarrow x = at,\ t \in K_{a^{-1}a} \cap K_{b^{-1}b}, \\ &\Longrightarrow x = at,\ t = a^{-1}at,\ t = b^{-1}bt \\ &\Longrightarrow x = at,\ at = a^{-1}a(at),\ at = b^{-1}b\left(at\right) \\ &\Longrightarrow x = a^{-1}ax,\ x = b^{-1}bx \Longrightarrow x \in K_{a^{-1}a} \cap K_{b^{-1}b}, \end{aligned}$$

cioè:

$$T_a\left(K_{a^{-1}a} \cap K_{b^{-1}b}\right) \subseteq K_{a^{-1}a} \cap K_{b^{-1}b}. \tag{38}$$

Dalle (37) e (38) si ottiene la (35) (in forza delle (28) e (21)).

Per la (24) si ha:

$$K_{ab(ab)^{-1}} = K_{aa^{-1}bb^{-1}}. \tag{39}$$

La (33) (in forza delle (34), (35) e (39)) si scrive:

$$T_a \circ T_b : x \in K_{ab(ab)^{-1}} \longmapsto abx \in K_{ab(ab)^{-1}}.$$

Essa coincide con T_{ab}, quindi:

$$T_{ab} = T_a \circ T_b. \tag{40}$$

Si consideri l'applicazione:

$$\phi : a \in K \longmapsto T_a \in \mathscr{T}.$$

Essa è biettiva (per la (30)) e, per la (40), risulta un omomorfismo del gruppide moltiplicativo di K sul gruppide di trasformazioni parziali $\mathscr{T}$ di K.

Dunque, l'applicazione ϕ è un isomorfismo tra i gruppidi $(K,\cdot)$ e $(\mathscr{T},\circ)$.

Si consideri la famiglia $\{K_e\}_{e\in\mathscr{U}}$. Essa gode delle seguenti proprietà.

$$\forall a \in K, \quad \bigcap_{e\in\mathscr{U}_a} K_e = K_{aa^{-1}},$$

dove $\mathscr{U}_a = \{e \in \mathscr{U} : a \in K_e\}$. Infatti:

$$\begin{aligned} a \in K_e \quad &\Longrightarrow \quad aa^{-1} \in K_e \Longrightarrow K_{aa^{-1}} \subseteq K_e \\ &\Longrightarrow \quad K_{aa^{-1}} \subseteq \bigcap_{e\in\mathscr{U}_a} K_e \subseteq K_{aa^{-1}} \Longrightarrow \bigcap_{e\in\mathscr{U}_a} K_e = K_{aa^{-1}}. \end{aligned}$$

Osserviamo che per ogni $a \in K$, $K_{aa^{-1}}$ è l'ideale generato da a. Infatti, denotato con (a) tale ideale, si ha $e = a^{-1}a \in (a)$ e quindi $\alpha e \in (a)$, $\forall \alpha \in K$, onde $K_e \subseteq (a)$. D'altra parte $a \in K_e$, quindi abbiamo anche l'altra inclusione $(a) \subset K_e$. Dunque $(a) = K_{aa^{-1}}$.

6. Endomorfismi di un corpide

Sia K un corpide qualsiasi. Si consideri l'applicazione

$$F_a : x \in K \longmapsto ax \in K, \qquad a \in K. \tag{41}$$

Si ha:

$$F_a(x+y) = a(x+y) = ax + ay = F_a(x) + F_a(y).$$

Dunque, F_a è un endomorfismo di $(K,+)$. Si ha:

$$\ker F_a = \{x \in K : ax = 0\}.$$

Dunque $\ker F_a$ coincide con l'ideale bilatero (cfr (23)) dei divisori dello zero di a. Inoltre:

$$\operatorname{Im} F_a = \{ax\}_{x\in K},$$

cioè $\operatorname{Im} F_a$ è l'ideale destro generato da a. Si ha:

$$\operatorname{Im} F_a = \{ax\}_{x\in K} = K_{aa^{-1}}. \tag{42}$$

Infatti,

$$e = aa^{-1} \in \operatorname{Im} F_a;$$

$$\alpha \in K_e \Longleftrightarrow \alpha = \alpha e = e\alpha = a\left(a^{-1}\alpha\right) \Longrightarrow \alpha \in \operatorname{Im} F_a,$$

onde

$$K_e \subseteq \operatorname{Im} F_a;$$

$$\begin{aligned} \alpha \in \operatorname{Im} F_a &\Longleftrightarrow (\alpha = ax,\ x \in K) \\ &\Longrightarrow e\alpha = eax = \left(aa^{-1}\right)ax = ax = \alpha \Longrightarrow \alpha \in K_e, \end{aligned}$$

quindi

$$\operatorname{Im} F_a \subseteq K_e.$$

Dunque

$$K_e = \operatorname{Im} F_a.$$

Dalla (42) si ha che $\operatorname{Im} F_a$ è un ideale bilatero sottocorpide di K. Si ha poi che la restrizione di F_a a $K_{aa^{-1}}$ coincide con T_a:

$$F_a|_{K_{aa^{-1}}} = T_a, \tag{43}$$

dunque F_a è biettiva tra $K_{aa^{-1}}$ e $K_{aa^{-1}}$.

Proviamo che:

$$a, b \in K \qquad F_a = F_b \Longleftrightarrow a = b. \tag{44}$$

Dimostrazione.

$$F_a = F_b \Longrightarrow \operatorname{Im} F_a = \operatorname{Im} F_b.$$

Essendo $\operatorname{Im} F_a = \operatorname{Im} F_b$, da (43) e (30), segue $a = b$. Il viceversa è ovvio. □

La famiglia di endomorfismi di $(K,+)$ data da $\mathscr{F} = \{F_a\}_{a\in K}$ è propria, per la (44).

Si consideri l'applicazione

$$\phi : a \in K \longmapsto F_a \in \mathscr{F}.$$

Teorema 6.1. *Dato un corpide K, la famiglia propria $\mathscr{F} = \{F_a\}_{a\in K}$ di endomorfismi di $(K,+)$, definiti dalla (41), rispetto alla composizione di endomorfismi di $(K,+)$ e alla somma di endomorfismi di $(K,+)$ costituisce un corpide isomorfo a K. Gli idempotenti di $(\mathscr{F},+,\circ)$ sono quegli elementi $F \in \mathscr{F}$ tali che F ristretta a $\operatorname{Im} F$ è l'identità. Lo zero di $(\mathscr{F},+,\circ)$ è l'endomorfismo nullo $F_0 = \underline{0}$. $F \in \mathscr{F}$ non è un divisore dello zero se, e soltanto se, esso è un automorfismo di $(K,+)$.*

Dimostrazione. La famiglia $\mathscr{F}$ è chiusa rispetto alla composizione di endomorfismi di $(K,+)$. Infatti, per ogni F_a e F_b, poiché

$$F_a \circ F_b : x \in K \longmapsto abx \in K,$$

si ha $F_a \circ F_b = F_{ab} \in \mathscr{F}$. Inoltre $\mathscr{F}$ è chiuso rispetto alla somma di endomorfismi:

$$\forall F_a, F_b \in \mathscr{F}, \qquad F_a + F_b = F_{a+b}, \tag{45}$$

perché

$$F_a(x) + F_b(x) = ax + bx = (a+b)\,x \in K. \tag{46}$$

Dalle (45) e (46) si ricava che:

$$\begin{aligned} \phi(ab) &= \phi(a) \circ \phi(b), \\ \phi(a+b) &= \phi(a) + \phi(b). \end{aligned}$$

Dunque

$$\phi : K \longrightarrow \mathscr{F}$$

è un isomorfismo del corpide $(K,+,\cdot)$ sul sistema $(\mathscr{F},+,\circ)$ a doppia composizione. Ne segue che $(\mathscr{F},+,\circ)$ è un corpide isomorfo a $(K,+,\cdot)$. Gli idempotenti di $(\mathscr{F},+,\circ)$ sono quegli endomorfismi F di $\mathscr{F}$ la cui restrizione a $\operatorname{Im} F$ risulta l'identità. Inoltre, se F è un automorfismo di $(K,+)$ e si ha $F \circ G = \underline{0}$, con $G \in \mathscr{F}$, per ogni $u \in K - \{0\}$, deve risultare $G(u) = 0$, altrimenti $F(G(u)) \neq 0$, dunque $G = 0$, onde F non è divisore dello zero. Viceversa, sia F^{-1} l'applicazione inversa di F, esistente perché F non è un divisore dello zero (vedi [2], Teorema 2.4) del corpide $(\mathscr{F},+,\circ)$. Si ha $F \circ F^{-1} = \mathscr{U}$, dove $\mathscr{U}$ è l'unità di $\mathscr{F}$, cioè l'automorfismo identico di $(K,+)$. Ma allora l'applicazione F di K in se ammette l'applicazione inversa e quindi è una biezione, cioè è un automorfismo. □

Ne segue che $(\mathscr{F},+,\circ)$ non è unitario se, e soltanto se, è privo di automorfismi.

BIBLIOGRAFIA

[1] M. Scafati Tallini - M. Iurlo, *Su una classe notevole di anelli*, Quaderni del Seminario di Geometria Combinatoria "Giuseppe Tallini" n. 156, Dipartimento di Matematica "Guido Castelnuovo", Università degli Studi di Roma "Sapienza", Novembre 2007.

[2] M. Scafati Tallini - M. Iurlo, *Studio di una classe notevole di anelli dotata di inverso generalizzato*, Le Matematiche **63** (2) (2008), 39-56.

[3] M. Scafati Tallini - M. Iurlo, *Relazione d'ordine in un corpide*, Le Matematiche **64** (1) (2009), 47-56.

[4] G. Tallini, *Sulla struttura algebrica delle trasformazioni tra parti di un insieme*, Ann. Mat. (**4**) **71** (1966), 295-322.

MARIA SCAFATI TALLINI
Viale Ippocrate, 97
00161 Roma
e-mail: tallini@mat.uniroma1.it

MAURIZIO IURLO
Largo dell'Olgiata, 15/106/1C
00123 Roma
e-mail: maurizio.iurlo@istruzione.it