LE MATEMATICHE
Vol. LXIII (2008) – Fasc. II, pp. 39–56

STUDIO DI UNA CLASSE NOTEVOLE DI ANELLI DOTATA DI INVERSO GENERALIZZATO

MARIA SCAFATI TALLINI - MAURIZIO IURLO

We study a remarkable class of rings, which we call *corpids,* that is the rings, different from zero, $(K, +, \cdot)$, such that $(K, \cdot)$ is an inverse semigroup (or groupid, which is the name given by G. Tallini [4]). The inverse semigroup has been defined and called generalized group, indipendently by Viktor Vladimirovich Vagner [6] in the Soviet Union and by Gordon Preston in the Great Britain [3].

Sommario

Nel presente lavoro si studia una classe notevole di anelli, che chiameremo *corpidi*, cioè degli anelli, non ridotti al solo 0, $(K, +, \cdot)$, tali che $(K, \cdot)$ risulti essere un semigruppo inverso (o gruppide, secondo la denoninazione di G. Tallini in [4]). Un semigruppo inverso è un gruppoide associativo, in cui gli elementi idempotenti (cioè gli elementi che coincidono con i propri quadrati) sono permutabili e ogni elemento è dotato di inverso generalizzato (vedi (3)). Il semigruppo inverso è stato introdotto, con il nome di *gruppo generalizzato*, indipendentemente da Viktor Vladimirovich Vagner [6], in Unione Sovietica nel 1952, e da Gordon Preston [3] in Gran Bretagna nel 1954. Un gruppide rappresenta la struttura algebrica della totalità delle applicazioni tra parti di un insieme.
Nel lavoro si studiano proprietà e caratterizzazioni di tale struttura algebrica.

Entrato in redazione: 8 febbraio 2008

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

1. Richiami sui gruppidi

Si definisce *gruppide* un gruppoide $(\mathscr{G},\cdot)$ soddisfacente alle seguenti proprietà:

$$\forall a,b,c \in \mathscr{G}, \quad (ab)c = a(bc) \quad \text{(proprietà associativa)}; \tag{1}$$

$$e_1,e_2 \in \mathscr{G} : e_1^2 = e_1, e_2^2 = e_2 \Longrightarrow e_1e_2 = e_2e_1; \tag{2}$$

$$\forall a \in \mathscr{G} \quad \exists a^{-1} \in \mathscr{G} : aa^{-1}a = a, \ a^{-1}aa^{-1} = a^{-1}. \tag{3}$$

L'elemento a^{-1} si dice *inverside* (o *inverso generalizzato* o, semplicemente, *inverso*) di a.
Un elemento u di $\mathscr{G}$ tale che $u^2 = u$ si dice *idempotente.* L'insieme degli elementi idempotenti u sarà indicato con $\mathscr{U}$.

Si dice che $\mathscr{G}$ *è dotato di annullatore* se esiste un elemento, 0, detto *annullatore*, tale che, per ogni a di $\mathscr{G}$, si abbia

$$a0 = 0a = 0.$$

L'annullatore, se esiste, è unico. Si dimostrano le proposizioni seguenti ([4], Proposizioni I, II, III), che qui richiamiamo.

Proposizione 1.1. *Per ogni a di* $\mathscr{G}$, aa^{-1} *e* $a^{-1}a$ *risultano idempotenti. L'inverside di a è unico. Si ha poi*

$$a^3 = a \Longleftrightarrow a = a^{-1},$$

e, quindi, per ogni $u \in \mathscr{U}$, *si ha*

$$u = u^{-1}.$$

Proposizione 1.2. *Per ogni a di* $\mathscr{G}$ *risulta* $\left(a^{-1}\right)^{-1} = a$. *Per ogni* $a,b \in \mathscr{G}$ *risulta* $(ab)^{-1} = b^{-1}a^{-1}$.

Proposizione 1.3. *Un gruppide* $\mathscr{G}$ *è un gruppo se, e soltanto se, possiede un unico idempotente.*

Si ricorda che un gruppide rappresenta la struttura algebrica della totalità delle applicazioni tra parti di un insieme.

2. Corpidi. Definizione e prime proprietà

Definiamo *corpide* un anello $K = (K,+,\cdot)$, non ridotto al solo 0, i cui elementi rispetto all'operazione di moltiplicazione costituiscono un gruppide $(K,\cdot)$.

Il gruppide $(K,\cdot)$ risulta allora dotato di annullatore, tale essendo lo zero di K. Osserviamo che lo 0 di K ammette inverside $0^{-1} = 0$.

Un corpide si dice *unitario* se esso è un anello unitario, cioè se esiste un elemento u ($u \neq 0$) di K, tale che per ogni $a \in K$ si abbia

$$au = ua = a.$$

Evidentemente, u è un idempotente e non è né zero, né un divisore dello zero. Dalla Proposizione 1.3 segue:

Teorema 2.1. *Un corpide unitario con un solo idempotente non nullo è un corpo.*

Esempio 1. Si consideri la somma diretta $\mathbb{A}$ degli anelli $\{\mathbb{R}_n\}_{n\in\mathbb{N}}$, ($\mathbb{R}_n = \mathbb{R}$, $\mathbb{R}$ insieme dei numeri reali), dove per somma diretta si intende il sottoinsieme del prodotto diretto di anelli $\{\mathbb{R}_n\}_{n\in\mathbb{N}}$ ($\mathbb{N}$ insieme dei numeri naturali), in ciascun elemento del quale si abbia $r_n \neq 0_n$ soltanto per un numero finito di elementi di $\mathbb{N}$. La somma diretta $\mathbb{A}$ risulta avere la struttura di anello, in cui ogni elemento è un divisore dello zero, per cui $\mathbb{A}$ non è un corpo. Dimostriamo che invece $\mathbb{A}$ ha la struttura di corpide. Essendo $\mathbb{A}$ commutativo rispetto alla moltiplicazione, gli idempotenti sono ovviamente permutabili, quindi l'unica cosa che occorre dimostrare è che ogni elemento ammette inverside. Considerato l'elemento $(r_n)_{n\in\mathbb{N}} \in \mathbb{A}$, il suo inverside è dato dall'elemento $(\bar{r}_n)_{n\in\mathbb{N}}$ di $\mathbb{A}$ in cui $\bar{r}_n = 0$ per gli stessi valori di $n \in \mathbb{N}$ per i quali si ha $r_n = 0$ e in cui, per ognuno dei restanti valori di $n \in \mathbb{N}$ (per i quali si ha quindi $r_n \neq 0$ e $\bar{r}_n \neq 0$), si ha $\bar{r}_n = r_n^{-1}$, dove r_n^{-1} indica l'inverso di r_n. □

Esempio 2. Sia X un insieme non vuoto e $\mathscr{P}(X)$ sia l'insieme delle parti di X. Definiamo in $\mathscr{P}(X)$ le seguenti due operazioni:

$$A + B \stackrel{\text{def}}{=} (A \cup B) \cap \complement (A \cap B), \qquad A \cdot B \stackrel{\text{def}}{=} A \cap B.$$

Si vede facilmente che $(\mathscr{P}(X), +, \cdot)$ è un anello (commutativo) e che esso è anche un corpide. Infatti, è facile verificare che $(\mathscr{P}(X), \cdot)$ risulta essere un gruppide. La proprietà (2) è banalmente verificata. Per provare la proprietà (3), basta osservare che, per ogni $A \in \mathscr{P}(X)$, l'inverside è dato da A stesso. Infatti, si ha:

$$A \cdot A \cdot A = A \cap A \cap A = A.$$

Si noti che anche l'opposto di un elemento di $\mathscr{P}(X)$ è l'elemento stesso. Inoltre in questo anello ogni elemento è idempotente, cioè $A^2 = A \cdot A = A$, per ogni $A \in \mathscr{P}(X)$. Da quanto precede risulta che $(\mathscr{P}(X), +, \cdot)$ è un corpide ma (cfr Proposizione 1.3) non è un corpo. □

L'anello considerato nell'esempio precedente è un anello booleano (cioè un anello in cui ogni elemento è idempotente). Ogni anello booleano è un corpide:

infatti, un anello booleano è commutativo e ogni elemento ammette inverside (l'elemento stesso).

Si ha il risultato seguente.

Teorema 2.2. *Sia K un corpide unitario. Per ogni elemento idempotente, e, di K si ha che $u-e$ è ancora un idempotente. Inoltre risulta*

$$e(u-e)=0. \tag{4}$$

Quindi, se è $e\neq 0$, $e\neq u$, allora sia e che $u-e$ sono divisori dello zero. Ne segue che un idempotente diverso da zero e da un divisore dello zero coincide con u.

Dimostrazione. Si ha:

$$(u-e)^2=u^2-2eu+e^2=u-2eu+e=u-2e+e=u-e \tag{5}$$

e quindi $u-e$ è un idempotente. Inoltre, essendo $e^2=e$, si ha la (4). □

Osservazione 1. Osserviamo che in un corpide se e ed f sono due idempotenti, allora anche ef, $e-ef$ ed $e+f-ef$ sono idempotenti. La (5), quindi, può ottenersi come conseguenza del fatto che $e-ef$ ed ef sono idempotenti. □

Dai Teoremi 2.2 e 2.1 segue facilmente il seguente:

Teorema 2.3. *Un corpide unitario K, privo di divisori dello zero è un corpo.*

Dato un elemento x di un corpide unitario K, se esiste un $y\in K$, tale che

$$xy=u,$$

allora risulta

$$y=x^{-1}.$$

Infatti, $xy=u$ implica

$$xyx=x,\quad yxy=y,$$

da cui

$$y=x^{-1}.$$

Chiameremo *inverso* di $x\in K$, un elemento $y\in K$ tale che $xy=yx=u$.

Ovviamente, l'inverso di un elemento, se esiste, coincide con l'inverside. Da ciò segue che l'inverso di un elemento, se esiste, è unico.

Proviamo ora che

Teorema 2.4. *Sia K un corpide unitario. Un elemento x di K ammette inverso se, e soltanto se, non è né zero, né un divisore dello zero, l'inverso coincidendo con l'inverside x^{-1} di x. Dunque, gli unici elementi di K che non ammettono inverso sono lo zero e i divisori dello zero.*

Dimostrazione. Cominciamo con il provare che, se $y \in K$, $y \neq 0$ e non divisore dello zero, allora y^{-1} non è zero, né divisore dello zero. Infatti, si ha $y^{-1} \neq 0$, in quanto se fosse $y^{-1} = 0$, si avrebbe $y = 0^{-1} = 0$ (cfr Proposizione 1.2). Se fosse y^{-1} divisore dello zero, esisterebbe $z \in K$, $z \neq 0$, tale che $y^{-1}z = 0$ [oppure $zy^{-1} = 0$] onde (cfr Proposizione 1.2), si avrebbe $z^{-1}y = 0$ [oppure $y^{-1}z = 0$], cioè (essendo $z^{-1} \neq 0$, in quanto è $z \neq 0$) y sarebbe divisore dello zero, contro l'ipotesi.
Sia ora x un elemento di K, diverso da zero e non divisore dello zero, onde altrettanto accade per x^{-1}. L'elemento $e = xx^{-1}$ è un idempotente (cfr Proposizione 1.1), diverso da zero (in quanto sia x che x^{-1} sono diversi da zero e non sono divisori dello zero). Inoltre $e = xx^{-1}$ non è un divisore dello zero, poiché se lo fosse, dovrebbe esistere $z \in K$, $z \neq 0$, tale che $ze = 0$ [oppure $ez = 0$], cioè $z(xx^{-1}) = (zx)x^{-1} = 0$ [oppure $x(x^{-1}z) = 0$]. Essendo $zx \neq 0$ [oppure $x^{-1}z = 0$], si avrebbe che x^{-1} [oppure x] sarebbe o zero o un divisore dello zero, il che è escluso per ipotesi.
Ne segue che $e = xx^{-1}$ deve essere l'unità u di K (cfr Teorema 2.2). In modo analogo si prova che $x^{-1}x = u$. Si è cosí provato che se $x \in K$ non è né zero, né divisore dello zero, esso ammette inverso. Il viceversa essendo ovvio, ne segue l'asserto. □

Dal Teorema 2.4 segue quindi ancora che

- *un corpide unitario, privo di divisori dello zero, è un corpo.*

Infatti, in un siffatto corpide ogni elemento non nullo ammette inverso e quindi è un corpo.

3. Sottocorpidi. Divisori dello zero in un corpide

Chiameremo *sottocorpide* H del corpide K un qualunque sottoinsieme H di K il quale, rispetto alle operazioni di somma e prodotto definite in K, sia un corpide. Si prova facilmente il seguente

Teorema 3.1. *H è un sottocorpide di K se, e soltanto se, H è un sottoanello dell'anello K e inoltre se*

$$\forall x \in H, \quad x^{-1} \in H. \tag{6}$$

Teorema 3.2. *Se H è un sottocorpide del corpide unitario K e possiede un elemento $x \neq 0$ e non divisore dello zero in K, allora x ammette inverso (che coincide con l'inverside), il quale, per la (6), appartiene ad H e, quindi, H contiene l'unità u di K, che è unità anche per H.*

Dimostrazione. Infatti, se $x \in H$, $x^{-1} \in H$: ne segue che $xx^{-1} \in H$. Ma se $x \neq 0$ e non divisore dello zero, $xx^{-1} = u$ (per il Teorema 2.2), onde $u \in H$. □

Dunque, un sottocorpide H del corpide unitario K, se non contiene u, è costituito soltanto dallo zero e da divisori dello zero di K, i quali, però, non è detto che siano divisori dello zero in H.

Si noti che H può possedere una sua unità u' ($\neq u$). Per esempio, il corpide $K = \mathbb{Z}_6$ ammette come sottocorpide $H = \{0,2,4\}$ che ha come unità $u' = 4$ e che risulta essere un corpo (isomorfo a $\mathbb{Z}_3$).

Sia ora K un corpide non necessariamente unitario. Denotiamo con $\mathscr{O}$ l'insieme costituito dallo zero e dai divisori dello zero di K e con $\mathscr{U}$ l'insieme degli idempotenti di K.

Proviamo che

Teorema 3.3. *Sia K un corpide, non necessariamente unitario. L'insieme $K-\mathscr{O}$ o è vuoto, ovvero è un gruppo rispetto al prodotto, l'inverso di $x \in K-\mathscr{O}$ essendo l'inverside x^{-1} di x in K.*

Dimostrazione. Proviamo che $K-\mathscr{O}$ ($\neq \emptyset$) è chiuso rispetto al prodotto, cioè che

$$x, y \in K-\mathscr{O} \Longrightarrow xy \in K-\mathscr{O}.$$

Si tratta di provare che xy è diverso da zero e non è un divisore dello zero. Ora, xy è manifestamente diverso da zero, poiché x e y non sono né zero né divisori dello zero. Resta da escludere che xy sia un divisore dello zero. Se cosí fosse, esisterebbe $z \in \mathscr{O} - \{0\}$, tale che $(xy)z = 0$ [oppure $z(xy) = 0$]. Si ha $yz \neq 0$, poiché $y \in K-\mathscr{O}$ e $z \neq 0$. Ma allora, essendo $x(yz) = 0$, x sarebbe un divisore dello zero, contro l'ipotesi [analogamente si ragiona se è $z(xy) = 0$].
Dunque, $K-\mathscr{O}$ è chiuso rispetto al prodotto. Proviamo ora che:

$$\forall x, y \in K-\mathscr{O}, \quad xx^{-1} = yy^{-1}. \tag{7}$$

Si ha posto $z = xx^{-1} - yy^{-1}$:

$$\begin{aligned} y^{-1}zx &= y^{-1}\left(xx^{-1} - yy^{-1}\right)x = \\ &= y^{-1}\left(xx^{-1}x\right) - \left(y^{-1}yy^{-1}\right)x = \\ &= y^{-1}x - y^{-1}x = 0. \end{aligned}$$

Poiché si ha $x \in K-\mathscr{O}$, si ha

$$\left(y^{-1}z\right)x = 0 \Longrightarrow y^{-1}z = 0 \Longrightarrow \left(y^{-1}z\right)^{-1} = z^{-1}y = 0.$$

Quindi, essendo $y \in K-\mathscr{O}$, risulta $z^{-1} = 0$, cioè $z = 0$. Si è cosí provata la (7). Osserviamo ora che, se $x \in \mathscr{K} - \mathscr{O}$, allora $x^{-1} \in K-\mathscr{O}$. Infatti, altrimenti x^{-1} sarebbe un divisore dello zero, cioè esisterebbe un elemento $z \in \mathscr{O} - \{0\}$, tale che $x^{-1}z = 0$ [oppure $zx^{-1} = 0$], ossia $xz^{-1} = 0$ [oppure $z^{-1}x = 0$] e quindi $z^{-1} = 0$ (perché $x \in K-\mathscr{O}$), cioè $z = 0$, contro l'ipotesi. Se nella (7) si pone $y = x^{-1}$, si ha:

$$xx^{-1} = x^{-1}x \in K-\mathscr{O}, \qquad \forall x \in K-\mathscr{O}.$$

Posto

$$u = xx^{-1} = x^{-1}x \in K-\mathscr{O}, \quad \forall x \in K-\mathscr{O},$$

si ha che u non dipende da x, in forza della (7). Proviamo che u funge da unità di $K-\mathscr{O}$, cioè che

$$ux = xu = x, \qquad \forall x \in K-\mathscr{O}.$$

Si ha, per ogni $x \in K-\mathscr{O}$:

$$xx^{-1} = x^{-1}x = u \Longrightarrow xu = xx^{-1}x = x, \quad ux = xx^{-1}x = x.$$

Dunque, in $K-\mathscr{O}$ esiste l'elemento u che funge da unità e l'inverso di ogni elemento x, inverso che coincide con x^{-1}, onde l'asserto. □

Teorema 3.4. *Per ogni corpide K risulta*

$$\mathscr{U} - \{u\} \subseteq \mathscr{O}, \qquad u \in K-\mathscr{O},$$

essendo u l'unità del gruppo $K-\mathscr{O}$.

Dimostrazione. Poiché $K-\mathscr{O}$ è un gruppo rispetto al prodotto, l'unico idempotente di $K-\mathscr{O}$ è l'unità, u, di $K-\mathscr{O}$, quindi gli idempotenti di K, distinti da u, appartengono a $\mathscr{O}$, onde l'asserto. □

Dal Teorema 3.3 segue subito che

Teorema 3.5. *Un corpide che non possiede divisori dello zero è un corpo.*

Dimostrazione. Si ha $K - \mathscr{O} = K - \{0\}$ e quindi, per il Teorema 3.3, $K - \{0\}$ è un gruppo, pertanto K è un corpo. □

4. Ideali di un corpide

Definiamo *ideale* di un corpide $(K,+,\cdot)$, un ideale dell'anello $(K,+,\cdot)$.

Teorema 4.1. *Un ideale bilatero I di $(K,+,\cdot)$ è un sottocorpide di K.*

Dimostrazione. Basta provare che $\forall x \in I$, $x^{-1} \in I$ (cfr Teorema 3.1). Si ha

$$x \in I \Longrightarrow x^{-1}x \in I \Longrightarrow \left(x^{-1}x\right)x^{-1} = x^{-1} \in I. \qquad \square$$

Teorema 4.2. *Un sottocorpide H del corpide unitario K, tale che sia $H-\mathscr{O} \neq \emptyset$, contiene l'elemento u, unità del gruppo $K-\mathscr{O}$, risultando $H-\mathscr{O}$ un sottogruppo di $K-\mathscr{O}$. Inoltre, anche il corpide H è unitario e ammette la stessa unità del corpide K.*

Dimostrazione. Sia H un sottocorpide del corpide unitario K, tale che $H-\mathscr{O} \neq \emptyset$. Evidentemente $H-\mathscr{O} \subseteq K-\mathscr{O}$. Inoltre $H-\mathscr{O}$ è chiuso rispetto al prodotto. Infatti, se $x,y \in H-\mathscr{O}$, si ha $xy \in H$ (in quanto H è chiuso rispetto al prodotto) e $xy \in K-\mathscr{O}$ (in quanto $H-\mathscr{O} \subset K-\mathscr{O}$ e $K-\mathscr{O}$ è chiuso rispetto al prodotto), quindi $xy \in H-\mathscr{O}$. Per il Teorema 3.3 (per $K=H$) si ha che $H-\mathscr{O}$ è un gruppo, sottogruppo di $K-\mathscr{O}$ e quindi se $x \in H-\mathscr{O}$ allora $x^{-1} \in H-\mathscr{O}$ e $xx^{-1} = u \in H-\mathscr{O}$ dove u è l'unità del gruppo moltiplicativo $K-\mathscr{O}$, quindi $H-\mathscr{O}$ è sottogruppo di $K-\mathscr{O}$. Se K è unitario, la sua unità è quella del gruppo $K-\mathscr{O}$, ma allora u deve appartenere ad $H-\mathscr{O}$ e quindi ad H, che risulta anch'esso unitario, con la stessa unità di K. $\square$

Dai Teoremi 4.1 e 4.2 si ha subito il risultato seguente.

Teorema 4.3. *Gli ideali bilateri propri di un corpide unitario K sono tutti contenuti in $\mathscr{O}$.*

Dimostrazione. Ovviamente, un ideale bilatero proprio I di K non deve contenere u (infatti un ideale bilatero proprio di un anello non deve contenere l'unità). Inoltre, si ha $I \subseteq \mathscr{O}$, in quanto, se esistesse $x \in I$, $x \notin \mathscr{O}$, si avrebbe $u \in I$, il che è escluso (cfr Teorema 3.2). $\square$

È immediato provare che

Teorema 4.4. *Se I è un ideale bilatero di un corpide K, l'anello quoziente K/I risulta un corpide, che diremo* corpide quoziente *di K rispetto a I, l'inverside della classe $[x] = x+I$, $x \in K$, essendo la classe $[x^{-1}]$. Se K è unitario, anche K/I è unitario, l'unità essendo data da $[u]$.*

Si osservi che, in generale, $\mathscr{O}$ non è un ideale di K, come mostra il seguente esempio.

Esempio 3. Sia $K = \mathbb{Z}_6$, corpide unitario commutativo. In questo caso, $\mathscr{O}$ risulta essere costituito dagli elementi [0], [2], [3], [4] e si ha $[3]-[2]=[1] \notin \mathscr{O}$. □

Teorema 4.5. *Se $\mathscr{O}$ è un ideale bilatero di K ed è $K-\mathscr{O} \neq \emptyset$, allora $K/\mathscr{O}$ è un corpo.*

Dimostrazione. Infatti, per ogni $x \in K-\mathscr{O}$, si ha $[x][x^{-1}] = [xx^{-1}] = [u] = [x^{-1}x] = [x^{-1}][x]$, u essendo l'unità del gruppo moltiplicativo di $K-\mathscr{O}$, cioè ogni elemento non nullo di $K/\mathscr{O}$ ammette inverso. □

5. Caratteristica di un corpide

Chiameremo *caratteristica* di un corpide unitario K il periodo $p \geq 2$ di u.

Teorema 5.1. *Se p è finito, ogni elemento non nullo di K ha periodo dato da un divisore di p.*

Dimostrazione. Infatti, per ogni $x \in K-\mathscr{O}$, risulta

$$px = pu \cdot x = 0,$$

onde il periodo s di x è tale che $s \leq p$. Dividendo p per s, si ha $p = sq + r$, con $r < s$. Si deve però avere $r = 0$, perché se fosse $r > 0$, si avrebbe

$$0 = px = qu \cdot sx + rx,$$

da cui

$$0 = 0 + rx,$$

cioè

$$rx = 0,\ r < s.$$

Ma ciò è assurdo, quindi $r = 0$, onde $p = sq$, cioè l'asserto. □

Dal teorema precedente segue che

Teorema 5.2. *Se la caratteristica, p, di un corpide è un numero primo, allora ogni elemento non nullo di K ha periodo p.*

Teorema 5.3. *Se il corpide unitario K ha caratteristica 2, l'insieme $\mathscr{U}$ degli idempotenti di K è un sottocorpide di K.*

Dimostrazione. Per ogni $\varepsilon, \eta \in \mathscr{U}$,

$$\varepsilon\eta \in \mathscr{U},$$

$$(\varepsilon+\eta)^2 = \varepsilon^2+\eta^2+2\varepsilon\eta = \varepsilon+\eta \in \mathscr{U}.$$

Inoltre, per ogni $\varepsilon \in \mathscr{U}$

$$\left[\varepsilon = \varepsilon\varepsilon^{-1}\varepsilon, \quad \varepsilon = \varepsilon^2\left(\varepsilon\varepsilon^{-1}\varepsilon\right)^2 = \varepsilon^2\left(\varepsilon^{-1}\right)^2\varepsilon^2 = \varepsilon\left(\varepsilon^{-1}\right)^2\varepsilon\right]$$
$$\Longrightarrow \left(\varepsilon^{-1}\right)^2 = \varepsilon^{-1} \Longrightarrow \varepsilon^{-1} \in \mathscr{U}.$$

Allora $\mathscr{U}$ è un sottocorpide di K (cfr Teorema 3.1). □

Teorema 5.4. *Se l'anello $\mathbb{Z}_p$ è un corpide, allora necessariamente p deve ammettere una scomposizione in fattori primi semplice (cioè ogni fattore primo deve comparire alla prima potenza).*

Dimostrazione. Se, per assurdo, fosse $p = s^2t$, si avrebbe $(st)u \neq 0$. Essendo, per ipotesi, $\mathbb{Z}_p$ un corpide, l'elemento $[st]$ di $\mathbb{Z}_p$ ammette inverside $[x]$ (dove $[x]$ indica la classe di x), per cui si avrebbe

$$[st]\,[x]\,[st] = [st],$$

da cui essendo $\mathbb{Z}_p$ commutativo,

$$\left[s^2t\right][t][x] = [st],$$

ma

$$\left[s^2t\right] = [0]$$

onde

$$[st] = [0],$$

il che è assurdo, perché $st < s^2t = p$. □

Teorema 5.5. *Se $\mathbb{Z}_p$ è tale che p ammette una scomposizione in fattori primi semplice, $\mathbb{Z}_p$ è un corpide.*

Dimostrazione. Sia $p = p_1 \ldots p_s$, con $p_1, \ldots, p_s$ primi e inoltre diversi tra loro. Ricordiamo che in un anello finito K (commutativo unitario) gli unici elementi che non ammettono inverso sono i divisori dello zero e lo zero stesso, cioè $K - \mathscr{O}$ coincide con l'insieme degli elementi che ammettono inverso e $\mathscr{O}$ con quello degli elementi che non ammettono inverso. D'altra parte, in $\mathbb{Z}_p$ l'insieme $K - \mathscr{O}$ coincide con l'insieme degli elementi $[h]$ per cui h sia primo con p. Dunque, se h è primo con p, allora $[h] \in K - \mathscr{O}$ e, quindi, ammette inverso, onde $[h]$

ammette inverside. Si tratta dunque solo di provare che, se h non è primo con p, allora $[h]$ ammette inverside $[k]$, il quale evidentemente deve appartenere a $\mathscr{O}$, altrimenti l'inverso di $[k]$, cioè $[h]$, dovrebbe esso pure appartenere a $K-\mathscr{O}$ e h risulterebbe primo con p. Se h non è primo con $p = p_1 p_2 \dots p_r p_{r+1} \dots p_s$ $(h < p)$ non è restrittivo supporre $h = \ell p_1 p_2 \dots p_r$, con ℓ primo con $p_{r+1} \dots p_s$, onde $(h,p) = p_1 p_2 \dots p_r$. Porremo $q = p_1 \dots p_r$, $q' = p_{r+1} \dots p_s$, onde $qq' = p$. Si ha poi $(h,q') = 1$, $(\ell,q') = 1$. Si tratta di determinare un intero k, con $1 < k < p$, tale che

$$[h]\,[k]\,[h] = [h], \quad [k]\,[h]\,[k] = [k],$$

cioè

$$h^2 k \equiv h \bmod p, \quad k^2 h \equiv k \bmod p.$$

Essendo $h = \ell q$, si tratta di determinare k $(1 < k < p)$ tale che

$$\ell^2 q^2 k \equiv \ell q \bmod p, \quad k^2 \ell q \equiv k \bmod p,$$

cioè tale che

$$\ell q\,(\ell q k - 1) = a q q', \quad k\,(\ell q k - 1) = b q q', \quad a,b \in \mathbb{Z}.$$

Poiché ℓ è primo con q', la prima delle due relazioni precedenti risulta equivalente a:

$$\ell q k - 1 = c q', \quad c = \frac{a}{\ell} \in \mathbb{Z}.$$

Dunque, si tratta di determinare k $(1 < k < p)$ e gli interi b, c, tali che:

$$\ell q k - 1 = c q', \quad k c = b q. \tag{8}$$

In $\mathbb{Z}_{q'}$, l'equazione $[\ell q^2]\,[x] = [1]$ ammette soluzione, in quanto ℓq^2 è primo con q' (perché $(\ell,q') = 1$, $(q,q') = 1$ e, quindi, anche $(q^2,q') = 1$). Sia $[\overline{d}]$ una tale soluzione, $1 \le \overline{d} < q'$, onde $\ell q^2 \overline{d} - 1 \equiv 0 \bmod q'$, ossia esiste $\overline{c}$, $\overline{c} \in \mathbb{Z}$, tale che $\ell q^2 \overline{d} - 1 = \overline{c} q'$. Posto $\overline{k} = q\overline{d}$ $(< p)$, si ha $\ell q \overline{k} - 1 = \overline{c} q'$ e inoltre

$$\overline{k}\overline{c} = \overline{c}\overline{d} q.$$

Se si pone infine $\overline{b} = \overline{c}\overline{d}$ si ottiene la soluzione $\overline{k}$, $\overline{b}$, $\overline{c}$ del sistema (8), onde l'asserto. □

Dai Teoremi 5.4 e 5.5 si ha quindi la seguente caratterizzazione dei corpidi.

- *Un anello $\mathbb{Z}_p$ è un corpide se, e soltanto se, p è fattorizzabile in fattori primi diversi tra loro.*

In modo del tutto analogo, piú in generale, si prova che

Teorema 5.6. *Se A è un anello (commutativo unitario) euclideo e $p \in A - \{0\}$ è un elemento fattorizzabile in fattori primi diversi tra loro, l'anello $A/(p)$ è un corpide unitario e viceversa.*

6. Altri risultati sui corpidi

Sia K un corpide unitario e $\mathscr{U}$ l'insieme dei suoi idempotenti. Supponiamo $|\mathscr{U}| \leq 5$. Allora K possiede l'unità u e quindi $0, u \in \mathscr{U}$, onde $|\mathscr{U}| \geq 2$. Se $|\mathscr{U}| = 2$, cioè se $\mathscr{U} = \{0, u\}$, allora K è un corpo (cfr Teorema 2.1). Supponiamo $|\mathscr{U}| \geq 3$. Sia $e \in \mathscr{U}$, con $e \neq 0$, $e \neq u$. Si ha (cfr Teorema 2.2)

$$u - e \in \mathscr{U}.$$

Inoltre,

$$u - e \neq 0, \quad u - e \neq u, \quad u - e \neq e.$$

Infatti, le prime due disuguaglianze essendo ovvie, dimostriamo la terza. Si ha:

$$u - e = e \Rightarrow (u-e)^2 = u - e = e(u-e) = e - e^2 = e - e = 0 \Rightarrow u = e.$$

Ne segue che $\mathscr{U}$ contiene 4 idempotenti distinti: $0, u, e, u-e$, onde $|\mathscr{U}| \geq 4$. Se fosse $|\mathscr{U}| = 5$, esisterebbe un $\eta \in \mathscr{U}$ con $\eta \neq 0, u, e, u-e$. Ma allora $u - \eta \in \mathscr{U}$ con $u - \eta \neq 0$, $u - \eta \neq u$, $u - \eta \neq e$, $u - \eta \neq u - e$, onde $\mathscr{U}$ possiederebbe 6 elementi distinti. Dunque $|\mathscr{U}| \leq 5$ implica $|\mathscr{U}| = 2$, K corpo, oppure $|\mathscr{U}| = 4$.

Supponiamo ora $|\mathscr{U}| = 4$. Si ha il risultato seguente.

Teorema 6.1. *Un corpide K con esattamente* 4 *idempotenti, ciascuno permutabile con ogni elemento di K, è isomorfo alla somma diretta di due corpi.*

Dimostrazione. Sia $|\mathscr{U}| = 4$. Posto $\eta = u - e$, si ha $\mathscr{U} = \{0, u, e, \eta\}$. Si ha, per $a \in K - \{0\}$, con $a = ae$:

$$a = ae \Leftrightarrow a^{-1}a = e \Leftrightarrow a\eta = 0 \Leftrightarrow a^{-1} = ea^{-1} \Leftrightarrow \eta a^{-1} = 0. \tag{9}$$

Infatti

$$a = ae \Rightarrow a^{-1}a = a^{-1}ae,$$

ma si ha

$$a^{-1}a \neq 0,$$

in quanto

$$a^{-1}a = 0 \Rightarrow a\left(a^{-1}a\right) = a \cdot 0 \Rightarrow a \cdot 0 = a \Rightarrow a = 0,$$

il che è assurdo, in quanto $a \in K - \{0\}$. Si ha ancora

$$a^{-1}a \neq u,$$

in quanto

$$a^{-1}a = u \Rightarrow a^{-1}a(u-e) = u - e \Rightarrow a^{-1}(a - ae) = 0 = u - e$$

e si ha inoltre

$$a^{-1}a \neq \eta,$$

in quanto

$$a^{-1}a = \eta = u - e \Rightarrow a = a^{-1}aa = a - ae = 0.$$

In modo analogo si dimostra, per $a \in K - \{0\}$:

$$a = ea \Leftrightarrow aa^{-1} = e \Leftrightarrow \eta a = 0 \Leftrightarrow a^{-1} = a^{-1}e \Leftrightarrow a^{-1}\eta = 0. \qquad (10)$$

Si consideri ora $K_e = \{b \in K : b = be\}$, $K_\eta = \{c \in K : c = c\eta\}$. Si ha:

$$K_e \cap K_\eta = \{0\}.$$

Infatti

$$a \in K_e \cap K_\eta \Rightarrow a = ae = a\eta = a(u - e) = a - ae \Rightarrow a = ae = 0.$$

Supponiamo che e sia permutabile con ogni elemento di K, onde anche η è tale. Allora K_e e K_η sono sottocorpidi di K. Infatti, essi sono evidentemente sottoanelli; proviamo che $a \in K_e \Rightarrow a^{-1} \in K_e$. Si ha:

$$a \in K_e \Rightarrow a = ae \Rightarrow a^{-1} = ea^{-1} = a^{-1}e \Rightarrow a^{-1} \in K_e.$$

Proviamo che K_e è un corpo che ammette come unità e (analogamente per K_η). Essendo

$$a = ae \Leftrightarrow a^{-1}aa^{-1} = a^{-1} = a^{-1}aea^{-1} = ea^{-1}aa^{-1} = ea^{-1},$$

si ha:

$$a \in K_e \Rightarrow a = ae = ea$$

e dunque e è unità di K_e. D'altra parte, per le (9) e (10), si ha, $\forall a \in K - \{0\}$:

$$a^{-1}a = e$$

e

$$a^{-1} = ea^{-1} = a^{-1}e \Rightarrow aa^{-1} = e.$$

E analogamente per K_η. Pertanto K_e e K_η sono corpi. Consideriamo dunque i corpi K_e e K_η e sia

$$H = K_e \oplus K_\eta.$$

Si consideri

$$\varphi : a \in K \longmapsto (ae, a\eta) \in H = K_e \oplus K_\eta.$$

Proviamo che φ è un omomorfismo dell'anello K nell'anello H. Si ha:

$$\begin{aligned}\varphi(a+b) &= ((a+b)e,(a+b)\eta) = (ae,a\eta)+(be,b\eta) = \varphi(a)+\varphi(b),\\ \varphi(ab) &= (abe,ab\eta) = (ae,a\eta)(be,b\eta) = \varphi(a)\varphi(b),\end{aligned}$$

onde l'asserto. Mostriamo che $\ker\varphi = \{0\}$ e $\operatorname{Im}\varphi = H$, cioè che φ è un isomorfismo.

$$a \in \ker\varphi \Rightarrow \varphi(a) = (ae,a\eta) = (0,0) \Rightarrow ae = 0 \Rightarrow a = 0,$$

cioè $\ker\varphi = \{0\}$. Si ha (cfr (9) e (10)):

$$(a,b) \in H \Rightarrow a = ae,\ b = b\eta \Rightarrow a\eta = 0,\ be = 0,$$

da cui

$$\varphi(a+b) = ((a+b)e,(a+b)\eta) = (ae+be,a\eta+b\eta) = (a,b),$$

onde $H \subseteq \operatorname{Im}\varphi$ e, quindi, essendo $\operatorname{Im}\varphi \subseteq H$, si ha $\operatorname{Im}\varphi = H$. □

Sia γ un campo, $\gamma[x]$ l'anello dei polinomi su γ, $f(x)$ un polinomio in $\gamma[x]$. Si consideri l'anello $K = K_f = \gamma[x]/(f)$. Si ha il risultato seguente.

Teorema 6.2. *L'anello $\gamma[x]/(f)$ è un corpide se, e soltanto se, f è semplice* (*cioè se f non ammette fattori primi multipli*).

Dimostrazione. [$\Longrightarrow$] Se n (≥ 1) è il grado di f, ogni elemento di K può essere individuato da un ben determinato polinomio di grado minore di n. Sia $f = s^2t$ ($s,t \in \gamma[x]$, $\deg s > 1$), $\deg st < n$, quindi $[st]$ ($\in K$) è non nullo ($\deg s$ indica il grado di s). Supposto K un corpide, determiniamo l'inverside di $[st]$. Esso sarà un $x \in K$ tale che $[st]\cdot[x]\cdot[st] = [st]$, ove $x = [g]$, $\deg g < n$, onde è

$$[st]\cdot[g]\cdot[st] = [st] = [s^2t]\cdot[gt] = [f][gt] = [0],$$

ossia,

$$[st] = [0],$$

ma ciò è escluso (perché $[st] \neq [0]$), onde l'asserto.
[$\Longleftarrow$] Proviamo ora che, se f è semplice, allora K_f è un corpide. Si tratta di provare che, per ogni $[a] \in K_f$, esiste un $[x] \in K_f$ tale che:

$$[a]\cdot[x]\cdot[a] = [a], \quad [x]\cdot[a]\cdot[x] = [x]. \tag{11}$$

Se il polinomio a è primo con f, ciò è immediato (infatti $ax + fy = 1 \implies [a]\cdot[x] = [1]$). Supponiamo dunque che a non sia primo con f e sia $d = (a,f)$.

Sarà $a = da_1$, $f = df_1$, con $(a_1, f_1) = 1$, $(d, f_1) = 1$ (si ha $(d, f_1) = 1$, in quanto f è semplice). Ne segue che $(a_1 d^2, f_1) = 1$. Esistono allora due polinomi α e β tali che:

$$a_1 d^2 \alpha + f_1 \beta = 1. \tag{12}$$

Posto $x = d\alpha$, moltiplicando ambo i membri della (12) una volta per $a = da_1$ e una volta per $x = d\alpha$ si ottiene:

$$a^2 x + f\beta a_1 = a, \quad x^2 a + f\alpha\beta = x. \tag{13}$$

Passando alle classi mod f, dalle (13) si hanno le (11). □

Teorema 6.3. *Sia K un corpide. Se esiste un elemento $\eta \in \mathscr{U}$, tale che*

$$\forall e \in \mathscr{U}, \quad \eta = e\eta \Rightarrow e = \eta,$$

allora K è unitario e ammette l'unità η e quindi η non è divisore dello zero.

Dimostrazione. Per ogni $e \in \mathscr{U}$, si ha (cfr Osservazione 1)

$$(e - \eta e + \eta) \in \mathscr{U}.$$

Si ha inoltre, per ipotesi,

$$\begin{aligned} \eta = (e - \eta e + \eta)\,\eta \quad &\Longrightarrow \quad e - \eta e + \eta = \eta \Longrightarrow \\ &\Longrightarrow \quad e - \eta e = 0 \Longrightarrow e = \eta e, \;\; e = e\eta. \end{aligned}$$

Poiché $\forall a \in K$, $aa^{-1} \in \mathscr{U}$ (cfr Proposizione 1.1), si ha $\forall a \in K$,

$$\begin{aligned} \left(aa^{-1} = \eta aa^{-1}, a^{-1}a = a^{-1}a\eta\right) \quad &\Rightarrow \quad \left(aa^{-1}a = \eta aa^{-1}a, aa^{-1}a = aa^{-1}a\eta\right) \\ &\Rightarrow \quad \left(a = \eta a, a = a\eta\right), \end{aligned}$$

onde l'asserto. □

Teorema 6.4. *Ogni corpide K per cui $\mathscr{U}$ è finito è unitario.*

Dimostrazione. Ragionando per assurdo, supponiamo K non unitario. Dalla proposizione precedente segue allora che per ogni idempotente e esiste un idempotente e', con $e = e'e$, tale che $e' \neq e$. Fissato un idempotente e_0, sia dunque e_1 un idempotente, tale che

$$e_0 = e_1 e_0, \quad \text{con } e_0 \neq e_1.$$

Sia poi e_2 un idempotente, tale che

$$e_1 = e_2 e_1, \quad e_1 \neq e_2.$$

Sia poi e_3 un idempotente, tale che

$$e_2 = e_3 e_2, \quad e_2 \neq$$

Così procedendo, si ottiene una successione di idempotenti $\{e_s\}_{s\in\mathbb{N}}$, tale che

$$e_{s-1} = e_s e_{s-1}, \quad e_{s-1} \neq e_s, \quad s = 1,2,\ldots \tag{14}$$

Dalla (14) si ottiene induttivamente:

$$e_h = e_s e_h, \quad 0 \leq h < s, \quad s = 1,2,\ldots \tag{15}$$

Proviamo che e_s è distinto da ogni e_t, con $t = 0,1,\ldots,s-1$. Poiché, per la (14), $e_s \neq e_{s-1}$, basta provare che $e_s \neq e_t$ per $t = 0,1,\ldots,s-2$. Se fosse $e_s = e_t$ (per $t = 0,1,\ldots,s-2$), avendosi per la (15) (con $s-1$ al posto di s):

$$e_t = e_{s-1} e_{t,} \quad t = 0,1,\ldots,s-2,$$

si avrebbe

$$e_s = e_t = e_{s-1} e_s = e_s e_{s-1} = e_{s-1}$$

(per la (14)), cioè

$$e_s = e_{s-1},$$

il che è escluso (per la (14)). Ne segue che la successione $\{e_s\}_{s\in\mathbb{N}}$ è costituita da elementi tutti distinti, cioè $\mathscr{U}$ è infinito, onde l'asserto. □

Come corollario si ha che:

Teorema 6.5. *Ogni corpide finito è unitario.*

Si noti che esistono corpidi non unitari (e quindi tali che $\mathscr{U}$ è infinito), come, per esempio, la somma diretta $\{\mathbb{R}_n\}_{n\in\mathbb{N}}$ (cfr Esempio 1). Esso è un corpide in cui ogni elemento è divisore dello zero e quindi non è unitario. Osserviamo anche che esistono corpidi unitari che posseggono sottocorpidi non unitari (per esempio il prodotto diretto di $\{\mathbb{R}_n\}_{n\in\mathbb{N}}$ che possiede come sottocorpide la somma diretta di $\{\mathbb{R}_n\}_{n\in\mathbb{N}}$) e, viceversa, corpidi non unitari che posseggono sottocorpidi unitari.

Teorema 6.6. *Un corpide con due soli idempotenti è un corpo.*

Dimostrazione. Essi devono essere necessariamente 0 e 1. Inoltre $\forall a \in K - \{0\}$, si ha $aa^{-1} = 1$, onde a non è divisore dello zero, cioè K è un corpo. □

Teorema 6.7. *Ogni corpide K, tale che $K - \mathscr{O}$ sia non vuoto, risulta unitario.*

Dimostrazione. Supponiamo $K - \mathscr{O} \neq \emptyset$. Si ha allora che $K - \mathscr{O}$ è un gruppo (cfr Teorema 3.3). Sia u la sua unità. Proviamo che u è unità per K, cioè

$$au = ua = a, \quad \forall a \in K. \tag{16}$$

La (16) è vera se $a \in K - \mathscr{O}$. Si tratta dunque di provare che

$$au = ua = a, \quad \forall a \in \mathscr{O}. \tag{17}$$

Si ha:

$$(ua - uau)u = uau - uau = 0, \quad \forall a \in \mathscr{O},$$

onde

$$(ua - uau)u = 0, \quad \forall a \in \mathscr{O}.$$

Poiché u non è un divisore dello zero ($u \in K - \mathscr{O}$), deve essere $ua - uau = 0$, ossia $u(a - au) = 0$ onde ancora $a - au = 0$, cioè $a = au$. Inoltre

$$\forall a \in \mathscr{O}, \quad u(au - uau) = 0 \Longrightarrow au - uau = 0 \Longrightarrow a = ua,$$

onde la (17). □

Teorema 6.8. *Se un corpide K ha ordine primo esso è isomorfo a $\mathbb{Z}_p$.*

Dimostrazione. Sia K un corpide ed e un suo idempotente non nullo. Consideriamo l'applicazione

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

Essa è un omomorfismo tra gli anelli $\mathbb{Z}$ e K, quindi $\mathbb{Z} / \ker \varphi$ è isomorfo a $\operatorname{Im} \varphi$, onde se e ha periodo infinito K contiene $\mathbb{Z}$. Se e ha periodo p, allora K contiene $\mathbb{Z}_p$. Se K è finito e ha ordine q, l'idempotente e ha periodo finito p, $(\mathbb{Z}_p, +)$ è un sottogruppo di $(K, +)$ e quindi p deve dividere q. Onde, se K ha ordine primo, esso è isomorfo a $\mathbb{Z}_p$. □

Teorema 6.9. *Se K è un corpide commutativo, ogni idempotente di periodo finito ha periodo semplice. In particolare se $\mathbb{Z}_p$ è un gruppide, p (che è il periodo dell'idempotente u) deve essere semplice.*

Dimostrazione. Sia p il periodo dell'idempotente e. Supponiamo che sia $p = st^2$ $(s, t \in \mathbb{N},\ s, t \geq 2)$. Si ha

$$ste \neq 0,$$

perché $st < st^2 = p$ e p è il periodo di e. Sia x l'inverside di ste. Si ha:

$$(ste)x(ste) = ste,$$

quidi, se K è commutativo, si ha

$$\left(s^2t^2e\right)x = ste,$$

onde, essendo

$$s^2t^2e = t\left(s^2te\right) = 0,$$

si ha

$$ste = 0,$$

il che è assurdo. Dall'assurdo trovato segue la tesi. □

BIBLIOGRAFIA

[1] A. H. Clifford - G.B. Preston, *The Algebraic Theory of Semigroups*, Math. Surv. Monogr. n. 7, vol.1 (1961), vol.2, American Mathematical Society, Providence, Rhode Island, 1967.

[2] K. R. Goodearl, *Von Neumann regular rings*, Pitman, London, San Francisco, 1979.

[3] G. B. Preston, *Inverse semi-groups*, J. London Math. Soc. **29** (1954), 396–403.

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

[5] J. von Neumann, *On regular rings*, Proc. Nat. Acad. Sci. U.S.A. (**23**) (1937), 341–347.

[6] V. V. Vagner, *Generalized groups*, Doklady Akad. Nauk SSSR **84** (1952), 1119–1122 (Russian).

MARIA SCAFATI TALLINI
Università "La Sapienza"
P.le A. Moro 5, 00185 Roma
e-mail: tallini@uniroma1.it

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