

RELAZIONE D'ORDINE IN UN CORPIDE

MARIA SCAFATI TALLINI - MAURIZIO IURLO

A corpid is a ring $(K, +, \cdot)$, different from zero, such that (K, \cdot) is an inverse semigroup. We define an order relation and the notion of simple element. By this we prove several results and a characterization of corpids.

Sommario

Definito un corpide K come un anello, non ridotto al solo 0, $(K, +, \cdot)$, tale che (K, \cdot) risulti essere un semigruppato inverso (o gruppato, secondo la denominazione di G. Tallini in [3]), si introduce ivi una relazione d'ordine e il concetto di elemento semplice, basato sulla relazione d'ordine introdotta. Si trovano vari risultati sui corpidi e caratterizzazioni dei corpidi stessi.

1. Richiami sui semigruppato inversi

Si richiamano la definizione e alcune propriet dei semigruppato inversi (cfr [2] e [3]).

Si definisce *semigruppato inverso* un gruppato (\mathcal{G}, \cdot) soddisfacente alle seguenti

Entrato in redazione: 25 novembre 2008

AMS 2000 Subject Classification: 16E50.

Keywords: ring, inverse semigroup.

proprietà:

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

$$e_1, e_2 \in \mathcal{G} : e_1^2 = e_1, e_2^2 = e_2 \implies e_1 e_2 = e_2 e_1; \quad (2)$$

$$\forall a \in \mathcal{G} \quad \exists a^{-1} \in \mathcal{G} : aa^{-1}a = a, \quad a^{-1}aa^{-1} = a^{-1}. \quad (3)$$

L'elemento a^{-1} si dice *inverside* (o *inverso generalizzato* o, semplicemente, *inverso*) di a .

Un elemento u di \mathcal{G} tale che $u^2 = u$ si dice *idempotente*. L'insieme degli elementi idempotenti u sarà indicato con \mathcal{U} .

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

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

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

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

Teorema 1.2. *Per ogni a di \mathcal{G} risulta $(a^{-1})^{-1} = a$. Per ogni $a, b \in \mathcal{G}$ risulta $(ab)^{-1} = b^{-1}a^{-1}$.*

Teorema 1.3. *In un semigrupp inverso G si ha, per $a, b \in G$:*

$$ab^{-1}a = a \implies ab^{-1}, b^{-1}a \in \mathcal{U}; \quad ab^{-1} = ba^{-1}; \quad b^{-1}a = a^{-1}b, \quad (4)$$

$$ab^{-1}a = a \iff aa^{-1}b = a \iff ba^{-1}a = a. \quad (5)$$

Dimostrazione. Risulta:

$$ab^{-1}a = a \implies (ab^{-1})(ab^{-1}) = ab^{-1},$$

onde ab^{-1} è un idempotente e quindi $(ab^{-1}) = (ab^{-1})^{-1} = ba^{-1}$. In modo analogo si prova che, se $ab^{-1}a = a$, risulta $b^{-1}a$ un idempotente e quindi $b^{-1}a = a^{-1}b$. Ne segue la (4).

Dalla (4) si ha:

$$ab^{-1}a = a \implies aa^{-1}b = a, \quad ba^{-1}a = a. \quad (6)$$

Inoltre, si ha:

$$\begin{aligned} aa^{-1}b = a &\implies b^{-1}aa^{-1}b = b^{-1}a \implies (b^{-1}a)(b^{-1}a)^{-1} = b^{-1}a \\ &\implies (b^{-1}a) = (b^{-1}a)(b^{-1}a)^{-1}(b^{-1}a) = (b^{-1}a)^2 \\ &\implies b^{-1}a \in \mathcal{U} \implies b^{-1}a = a^{-1}b, \end{aligned}$$

da cui:

$$aa^{-1}b = a \implies ab^{-1}a = a. \quad (7)$$

In modo analogo si prova che:

$$ba^{-1}a = a \implies ab^{-1}a = a. \quad (8)$$

Le (6), (7) e (8) equivalgono alla (5). \square

2. Relazione d'ordine in un corpide

Sia K un corpide e \mathcal{U} l'insieme dei suoi idempotenti. Poniamo $\mathcal{U}' = \mathcal{U} - \{0\}$. In K è definita la relazione \leq

$$a \leq b \iff ab^{-1}a = a, \quad (9)$$

la quale dimostreremo essere una relazione d'ordine.

Teorema 2.1. *Sia K un corpide. La relazione \leq in K , definita da*

$$a \leq b \iff ab^{-1}a = a,$$

è una relazione d'ordine.

Dimostrazione. Dimostriamo che la relazione data gode delle proprietà riflessiva, antisimmetrica e transitiva.

Proprietà riflessiva: per ogni $a \in K$ si ha

$$aa^{-1}a = a \iff a \leq a,$$

Proprietà antisimmetrica: per ogni $a, b \in K$ si ha

$$\begin{aligned} [a \leq b, b \leq a] &\iff [ab^{-1}a = a, ba^{-1}b = b] \\ &\iff [ab^{-1}a = a, b^{-1}ab^{-1} = b^{-1}] \iff a = b \end{aligned}$$

per l'unicità dell'inverso.

Proprietà transitiva: per ogni $a, b, c \in K$ si ha

$$\begin{aligned} [a \leq b, b \leq c] &\iff [ab^{-1}a = a, bc^{-1}b = b] \\ &\stackrel{(5)}{\implies} ac^{-1}a = (aa^{-1}b)c^{-1}(ba^{-1}a) = a(a^{-1}ba^{-1})a \\ &= aa^{-1}a = a \iff a \leq c. \end{aligned}$$

□

Osserviamo che se K è un corpo la relazione \leq si riduce all'identità. In tal caso infatti si ha:

$$a \leq b \iff ab^{-1}a = a \iff a = b.$$

Si ha:

$$e, \eta \in \mathcal{U}, \quad e \leq \eta \iff e\eta = e \quad (10)$$

Infatti: $[\implies]$ Se $e \leq \eta$, si ha

$$e\eta^{-1}e = e \implies ee\eta^{-1} = e \implies e^2\eta = e \implies e\eta = e.$$

$[\impliedby]$ Da $e\eta = e$ segue:

$$e^2\eta\eta^{-1}\eta = e \implies e\eta\eta^{-1}e\eta = e \implies e\eta^{-1}e = e \iff e \leq \eta.$$

Si ha inoltre:

$$\forall a \in K, \quad 0 \leq a \quad (11)$$

e, se K è unitario:

$$a \leq u \iff a^2 = a \iff a \in \mathcal{U}, \quad (12)$$

$$u \leq a \iff a^{-1} = u \iff a = u, \quad (13)$$

$$a \leq a^{-1} \iff a = a^3 \quad (14)$$

(cfr [3]). Dalle (12) e (13) si ha che se è $a \in K - \mathcal{U}$, allora a non è in relazione con u .

3. Idempotenti semplici

Un elemento α non nullo di K si dirà *semplice* se:

$$x \in K, \quad x \leq \alpha \implies [x = 0, \quad \text{ovvero} \quad x = \alpha]. \quad (15)$$

Teorema 3.1. *Se u è semplice, K è un corpo e viceversa.*

Dimostrazione. Sia u semplice. Se $x \in K$ è un idempotente, dalla (12) segue $x \leq u$. Ma allora $x = 0$, ovvero $x = u$. L'unico idempotente non nullo è quindi u , cioè K è un corpo (vedi [2], Teorema 2.1). Viceversa, se K è un corpo, cioè se u è l'unico idempotente non nullo (vedi [2], Teorema 2.1), da $x \leq u$ si ha $x \in \mathcal{U}$ (vedi (12)), e quindi $x = u$. Quindi è verificata la condizione

$$x \leq u \implies x = 0, \quad \text{ovvero} \quad x = u.$$

□

Si ha:

$$\forall e \in \mathcal{U}, \forall a \in K, \quad ea \leq a, \quad ae \leq a. \quad (16)$$

Infatti:

$$ea = e^2aa^{-1}a = eaaa^{-1}a = eaa^{-1}ea \iff ea \leq a.$$

Analogamente si dimostra $ae \leq a$.

Supponiamo $\alpha \in K$ semplice. Si ha:

$$\forall e \in \mathcal{U}, \quad e\alpha \leq \alpha \implies e\alpha = 0, \quad \text{ovvero} \quad e\alpha = \alpha, \quad (17)$$

$$\forall e \in \mathcal{U}, \quad \alpha e \leq \alpha \implies \alpha e = 0, \quad \text{ovvero} \quad \alpha e = \alpha.$$

Inoltre:

$$ea = 0, ae = a \implies a = 0, \quad e \in \mathcal{U}, a \in K, \quad (18)$$

$$e \in \mathcal{U}, a \in K, \quad ea = a, ae = 0 \implies a = 0. \quad (19)$$

Infatti:

$$(ea = 0, ae = a) \implies a(ea) = a^2 \implies a^2 = 0 \implies (e+a)^2 = e+a,$$

onde $e+a$ è un idempotente e quindi

$$(e+a)^{-1} = e+a;$$

$$[(e+a)e(e+a) = e+a, e(e+a) = e] \implies (e+a)^{-1} = e \implies a = 0.$$

Analogamente si ha la (19). Dalle (16), (17), (18) e (19) si ha (essendo α semplice):

$$\forall e \in \mathcal{U}, \quad e\alpha = \alpha e = 0, \quad \text{ovvero} \quad e\alpha = \alpha e = \alpha. \quad (20)$$

Sia $\{\theta_i\}_{i \in I} = \Theta$ l'insieme degli idempotenti semplici (e quindi non nulli) di K . Supponiamo Θ non vuoto, come accade per esempio se K è finito (vedi [2], Teorema 6.5). Da (20), si ha

$$\forall \theta \in \Theta, \forall e \in \mathcal{U}, \quad e\theta = \theta, \quad \text{ovvero} \quad e\theta = 0. \quad (21)$$

Proviamo che

Teorema 3.2. *Sia $t \in K - \{0\}$. Allora*

$$\forall e \in \mathcal{U}, \quad [et = t, \quad \text{ovvero} \quad et = 0] \implies t \text{ semplice}. \quad (22)$$

Dimostrazione. Infatti, se $\forall e \in \mathcal{U}$ si ha $et = t$, ovvero $et = 0$, allora per ogni $x \in K$ tale che $x \leq t$ si ha:

$$x \leq t \implies x = xtx \implies x^{-1} = x^{-1}xx^{-1} = (x^{-1}x)t(xx^{-1}) \implies x^{-1} = t$$

cioè $x = t$, ovvero $x = 0$. Ne segue che t è semplice. \square

Da (21) e (22), si ha:

$$\theta \in \mathcal{U}', \quad \theta \text{ semplice} \iff [\forall e \in \mathcal{U}, \quad e\theta = \theta \quad \text{ovvero} \quad e\theta = 0.] \quad (23)$$

Proviamo che:

Teorema 3.3. *Sia $\theta \in \mathcal{U}'$. Allora*

$$\theta \text{ semplice} \iff [\forall e \in \mathcal{U}, \quad e\theta \leq \theta \implies e = \theta, \quad \text{ovvero} \quad e = 0]. \quad (24)$$

Dimostrazione. $[\implies]$ Segue da (15).

$[\impliedby]$ Si ha

$$\forall e \in \mathcal{U}, \quad e\theta \leq \theta \stackrel{(24)}{\implies} [e = \theta, \quad \text{ovvero} \quad e\theta = 0] \stackrel{(23)}{\implies} \theta \text{ semplice.}$$

□

Dalla (24) si ha che

Teorema 3.4. *Se K ha un numero finito di idempotenti allora $\Theta \neq \emptyset$.*

Dimostrazione. Se K ha un numero finito di idempotenti allora K è unitario (cfr [2], Teorema 6.4). Allora $u \in \Theta$, $\Theta \neq \emptyset$. Infatti se $x \leq u$ allora $x = u$ oppure $x = 0$. Infatti

$$\begin{aligned} xu^{-1}x = x &\implies u^{-1} = x^{-1}, \text{ ovvero } x = 0 \\ &\implies u = x, \text{ ovvero } x = 0. \end{aligned}$$

Dalla (24) segue quindi che u è semplice. □

Teorema 3.5. *Si ha*

$$\alpha \text{ semplice} \iff \alpha^{-1} \text{ semplice.} \quad (25)$$

Dimostrazione. Sia α semplice:

$$\begin{aligned} x \leq \alpha^{-1} &\implies x^{-1} \leq \alpha \implies [x^{-1} = 0, \quad \text{ovvero} \quad x^{-1} = \alpha] \\ &\implies [x = 0, \quad \text{ovvero} \quad x = \alpha^{-1}] \end{aligned}$$

e quindi α^{-1} è semplice. □

Proviamo che:

Teorema 3.6. *Sia $\alpha \in K'$. Si ha:*

$$\alpha \text{ semplice} \iff [\forall e \in \mathcal{U}, \quad e\alpha = \alpha e = \alpha, \quad \text{ovvero} \quad e\alpha = \alpha e = 0]. \quad (26)$$

Dimostrazione. $[\implies]$ La condizione necessaria equivale alla (20).

$[\impliedby]$ Proviamo la condizione sufficiente. Si ha, dalla (26):

$$\begin{aligned} x \leq \alpha &\implies x^{-1}x \leq x^{-1}\alpha \implies x^{-1}x\alpha^{-1}xx^{-1}x = x^{-1}x\alpha^{-1}x \\ &\implies [x^{-1}x = \alpha^{-1}x, \quad \text{ovvero} \quad x^{-1}x = 0] \\ &\implies [x^{-1}xx^{-1} = \alpha^{-1}xx^{-1}, \quad \text{ovvero} \quad x = 0] \\ &\implies [x^{-1} = \alpha^{-1}, \quad \text{ovvero} \quad x = 0] \\ &\implies [x = \alpha, \quad \text{ovvero} \quad x = 0]. \end{aligned}$$

Si ha cosí la condizione sufficiente $[\impliedby]$. Il teorema cosí completamente dimostrato. \square

Si ha:

$$\theta_i\theta_j \in \Theta, \theta_i \neq \theta_j \implies \theta_i\theta_j = 0. \quad (27)$$

Infatti, posto nella (23) una prima volta $e = \theta_i$, $\theta = \theta_j$ e una seconda volta $e = \theta_j$, $\theta = \theta_i$, si ottiene $\theta_i = \theta_i\theta_j = \theta_j$, ovvero $\theta_i\theta_j = 0$, ma la prima uguaglianza è assurda essendo $\theta_i \neq \theta_j$, onde si ha $\theta_i\theta_j = 0$.

Sia A l'insieme degli elementi semplici di K e $A_0 = A \cup \{0\}$. Poniamo inoltre $\Theta_0 = \Theta \cup \{0\}$. Si ha

$$\alpha \in A_0 \iff \forall e \in \mathcal{U} \quad e\alpha = \alpha e = \alpha, \text{ ovvero } e\alpha = \alpha e = 0. \quad (28)$$

Dalla (28), da $e\alpha = \alpha e = \alpha$, ovvero $e\alpha = \alpha e = 0$, si ha $e\alpha\beta = \alpha e\beta = \alpha\beta$, ovvero $e\alpha\beta = \alpha e\beta = 0$. Ma ricordando che $\beta \in A_0$ e quindi $e\beta = \beta e$, si ottiene

$$\alpha, \beta \in A_0 \implies \forall e \in \mathcal{U}, e\alpha\beta = \alpha\beta e = \alpha\beta, \text{ ovvero } e\alpha\beta = \alpha\beta e = 0, \quad (29)$$

cioè

$$\alpha\beta \in \Theta_0.$$

Da (29) e (25) segue che (A_0, \cdot) è un sottogruppide di (K, \cdot) .

Dimostriamo ora che

Teorema 3.7. *Ogni corpide è privo di elementi nilpotenti.*

Dimostrazione. Sia K un corpide qualsiasi. Proviamo dapprima che

$$\alpha \in K, \alpha^2 = 0 \implies \alpha = 0. \quad (30)$$

Si ha

$$\begin{aligned} \alpha^2 = 0 &\implies [\alpha = \alpha\alpha^{-1}\alpha = \alpha e, \quad e = \alpha^{-1}\alpha \in \mathcal{U}] \\ &\implies [\alpha = \alpha e, \quad e\alpha = \alpha^{-1}\alpha^2 = 0] \\ &\implies [\alpha = \alpha e, \quad e\alpha = 0, \quad e \in \mathcal{U}] \\ &\stackrel{(18)}{\implies} \alpha = 0, \end{aligned}$$

onde la (30). Proviamo, piú in generale, che

$$\alpha \in K, \alpha^n = 0 \implies \alpha = 0. \quad (31)$$

Si ha:

$$\begin{aligned} \alpha^n = 0 &\implies e = \alpha^{-1}\alpha, \alpha = \alpha\alpha^{-1}\alpha = \alpha e \implies \\ e &\in \mathcal{U}, \alpha^{n-1} = \alpha^{n-1}e, e\alpha^{n-1} = \alpha^{-1}\alpha^n = 0 \implies \\ e &\in \mathcal{U}, \alpha^{n-1} = \alpha^{n-1}e, e\alpha^{n-1} = 0 \stackrel{18}{\implies} \alpha^{n-1} = 0, \end{aligned}$$

da cui si ha $\alpha^2 = 0$ e, per la (30), si ha la (31). \square

4. Corpidi e loro caratterizzazione

Sia K un corpide e sia Θ l'insieme dei suoi idempotenti semplici. Facciamo le seguenti ipotesi:

$$\Theta \neq \emptyset, \quad (32)$$

$$\forall a \in K, \forall \theta \in \Theta, \quad a\theta = \theta a, \quad (33)$$

$$\forall e \in \mathcal{U} - \{0\}, \quad \exists \theta \in \Theta : \theta \leq e. \quad (34)$$

Esempi di corpidi soddisfacenti alle (32), (33) e (34), si ottengono nel modo seguente. Sia $\{K_i\}_{i \in \mathcal{I}}$ una famiglia di corpi, sia $K = \otimes_{i \in \mathcal{I}} K_i$ e $H = \oplus_{i \in \mathcal{I}} K_i$ ($\subseteq K$). Ogni sottocorpide \bar{K} di K che contenga H soddisfa alle (32), (33) e (34). Si noti che, se \mathcal{I} è infinito, esistono dei sottocorpidi \bar{K} tali che $\bar{K} \neq K$, $\bar{K} \neq H$, intermedi tra K e H . Supponiamo, per esempio, \mathcal{I} infinito e $\gamma = K_i$, per ogni $i \in \mathcal{I}$ (γ corpo). Sia \bar{K} il sottoinsieme di $K = \otimes_{i \in \mathcal{I}} K_i$ ciascun elemento $(a_i)_{i \in \mathcal{I}}$ del quale sia quasi ovunque costante, cioè sia costante in $\mathcal{I} - \mathcal{F}$, dove \mathcal{F} è un sottoinsieme finito di \mathcal{I} (variabile elemento per elemento). Evidentemente \bar{K} è un sottocorpide di K , con $H \subseteq \bar{K} \subseteq K$, $\bar{K} \neq K$, $\bar{K} \neq H$.

Teorema 4.1. *Ogni corpide K soddisfacente alle (32), (33) e (34) è isomorfo a un sottocorpide \bar{K} di un prodotto diretto di corpi $\{K_i\}_{i \in \mathcal{I}}$, tale che $\bar{K} \supset \oplus_{i \in \mathcal{I}} K_i$.*

Dimostrazione. Sia K un corpide soddisfacente alle (32), (33) e (34). Per ogni $i \in \mathcal{I}$ sia $K_i = \{a\theta_i, a \in K, \theta_i \in \Theta\}$. L'insieme K_i è un corpo (sottocorpo di K) in virtù della (33), il quale ha come unità θ_i ($= \theta_i\theta_i$) e per inverso di $a\theta_i$ ($\neq 0$) l'elemento $a^{-1}\theta_i$. Infatti $(a^{-1}\theta_i)(a\theta_i) = a^{-1}a\theta_i = \theta_i$, ovvero $a^{-1}a\theta_i = 0$, ma tale eventualità è esclusa in quanto $a^{-1}a\theta_i = 0$ implica $a\theta_i = 0$, mentre $a\theta_i \neq 0$. Analogamente si prova $(a\theta_i)(a^{-1}\theta_i) = a^{-1}a\theta_i = \theta_i$. Si consideri l'applicazione;

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

Si ha (sempre per la (33)), per $a, b \in K$:

$$\begin{aligned}\varphi(a) &= \{a\theta_i\}_{i \in \mathcal{J}}, & \varphi(b) &= \{b\theta_i\}_{i \in \mathcal{J}}, \\ \varphi(a) + \varphi(b) &= \{(a+b)\theta_i\}_{i \in \mathcal{J}} = \varphi(a+b), \\ \varphi(a)\varphi(b) &= \{ab\theta_i\}_{i \in \mathcal{J}} = \varphi(ab).\end{aligned}$$

Dunque l'applicazione φ è un omomorfismo del corpide K nel corpide $\otimes_{i \in \mathcal{J}} K_i$.

Si ha:

$$a \in \ker \varphi \iff \varphi(a) = 0 \iff a\theta_i = 0, \forall i \in \mathcal{J}.$$

Posto $e = a^{-1}a \in \mathcal{U}$, se $e \neq 0$, per la (34), esiste un $\theta_{\bar{i}} \in \Theta$ tale che $\theta_{\bar{i}} = e\theta_{\bar{i}}$, cioè tale che $\theta_{\bar{i}} = a^{-1}a\theta_{\bar{i}}$. Dunque, se $a \in \ker \varphi$, cioè se $a\theta_i = 0$ per ogni $i \in \mathcal{J}$ e se $a \neq 0$, cioè se $e \neq 0$, sarà $\theta_{\bar{i}} = a^{-1}(a\theta_i) = 0$ il che è assurdo. Ne segue che $\ker \varphi = \{0\}$, onde φ è iniettiva e quindi K è isomorfo a $\varphi(K)$. Si ha (per la (27)), con $j \in I$, $\varphi(K_j) = \{a\theta_j\theta_i\}_{i \in \mathcal{J}} = \{a\theta_j, 0_i\}_{i \in \mathcal{J} - \{j\}} \subseteq \varphi(K)$. Ne segue che $\varphi(K)$ contiene $\otimes_{i \in \mathcal{J}} K_i$. \square

Si ha così il teorema seguente:

Teorema 4.2. *Un corpide K , soddisfacente alle (32), (33) e (34) è isomorfo a un sottocorpide \bar{K} prodotto diretto di una famiglia di corpi $\{K_i\}_{i \in \mathcal{J}}$ tale che $\bar{K} \supseteq \otimes_{i \in \mathcal{J}} K_i$.*

Come corollari si hanno i seguenti:

Teorema 4.3. *Un corpide K con Θ finito e non vuoto, soddisfacente alle (33) e (34) è isomorfo alla somma diretta di un numero finito di corpi.*

Teorema 4.4. *Un corpide K con \mathcal{U} finito e quindi Θ finito, soddisfacente alla (33), è somma diretta di un numero finito di corpi. In particolare, se K è commutativo ed \mathcal{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.*

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

MARIA SCAFATI TALLINI

Università La Sapienza

P.le A. Moro 5

00185 Roma, Italy

e-mail: tallini@mat.uniroma1.it

MAURIZIO IURLO

Istituto Superiore Luisa di Savoia

Via Luisa di Savoia 14

00100 Roma, Italy

e-mail: maurizio.iurlo@istruzione.it