

RENDICONTI *del* SEMINARIO MATEMATICO *della* UNIVERSITÀ DI PADOVA

CARLO TOFFALORI

Anelli regolari separabilmente chiusi

Rendiconti del Seminario Matematico della Università di Padova,
tome 71 (1984), p. 15-33

http://www.numdam.org/item?id=RSMUP_1984__71__15_0

© Rendiconti del Seminario Matematico della Università di Padova, 1984, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (<http://rendiconti.math.unipd.it/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques*
<http://www.numdam.org/>

Anelli regolari separabilmente chiusi.

CARLO TOFFALORI (*)

SUMMARY – A definition of separably closed regular ring (in a model-theoretic sense) is proposed in this paper. Consequently, we give a classification of complete theories of separably closed regular rings, and we study connections between separably closed regular rings and differentially closed regular rings.

1. Campi separabilmente chiusi.

Un campo A si dice separabilmente chiuso se è privo di ampliamenti algebrici separabili propri.

Se A ha caratteristica 0 , A è separabilmente chiuso se e solo se è algebricamente chiuso. Non altrettanto accade se la caratteristica di A è un primo p , in tal caso infatti A è separabilmente chiuso se e solo se, per ogni polinomio irriducibile $f(x) \in A[x]$, esiste $g(x) \in A[x]$ tale che $f(x) = g(x^p)$. Addirittura, si può dedurre

$$f(x) = x^{p^e} - a$$

per $e \in \mathbb{N}$, $a \in A$ opportuni. Si ottiene comunque una definizione intrinseca di campo algebricamente chiuso. Supponiamo allora di considerare campi di caratteristica fissata $p \neq 0$. Sia A un tale campo, e poniamo $A^p = \{a^p : a \in A\}$; A^p è sottocampo definibile di A , e si ha $A = A^p$ se e solo se A è perfetto (e, in tal caso, se A è separabilmente

(*) Indirizzo dell'A.: C. TOFFALORI: Istituto Matematico « U. Dini », Viale Morgagni 67/A, 50134 Firenze.

chiuso, A è anche algebricamente chiuso). In generale, comunque, si ha:

$$[A: A^p] = p^n$$

per $n \in \mathbf{N}$ opportuno, oppure

$$[A: A^p] = \infty.$$

Siano poi $a_1, \dots, a_n \in A$. Si dice che:

1) a_1, \dots, a_n sono p -indipendenti su A^p se i prodotti $a_1^{k_1} \dots a_n^{k_n}$ (con $0 \leq k_i < p$ per $i = 1, \dots, n$) sono linearmente indipendenti su A^p ;

2) a_1, \dots, a_n formano una p -base per A se sono p -indipendenti su A^p e, per ogni $b \in A$, a_1, \dots, a_n, b sono p -dipendenti su A^p .

Tali definizioni si possono agevolmente estendere a insiemi infiniti di elementi: si veda [4]. Si ha comunque:

(i) $[A: A^p] = p^n$ se e solo se A ammette una p -base di n elementi;

(ii) $[A: A^p] = \infty$ se e solo se, per ogni $n \in \mathbf{N}$, esistono in A n elementi p -indipendenti su A^p .

Si definisce allora l'invariante di Eršov di A , $\tau(A)$, nel modo seguente:

$$\tau(A) = \begin{cases} n & \text{se } [A: A^p] = p^n, \\ \infty & \text{altrimenti.} \end{cases}$$

TEOREMA 1.1 (Eršov, cfr. [3], [11]). Due campi separabilmente chiusi di caratteristica p aventi uguale invariante di Eršov sono elementarmente equivalenti.

Un linguaggio del 1° ordine adeguato a rappresentare le strutture sopra considerate può essere il seguente:

$$L = (+, \cdot, -, ^{-1}, 0, 1, (f_n)_{n \geq 1}, (\varepsilon_n)_{n \geq 0})$$

dove ciascun f_n è un simbolo funzionale n -ario, ed ogni ε_n è una costante individuale, e, in particolare, in ogni campo A , per ogni $n \geq 1$,

$a_1, \dots, a_n \in A$,

$$f_n^A(a_1, \dots, a_n) = \begin{cases} 1 & \text{se } a_1, \dots, a_n \text{ sono } p\text{-indipendenti su } A^p, \\ 0 & \text{altrimenti,} \end{cases}$$

e, per ogni $n \geq 0$,

$$\varepsilon_n^A = \begin{cases} 1 & \text{se } \tau(A) = n, \\ 0 & \text{altrimenti.} \end{cases}$$

Possiamo assiomatizzare opportunamente in L la classe dei campi di caratteristica p , ad esempio aggiungendo agli assiomi di campo gli enunciati degli schemi b), c) riportati nel successivo § 3; sia T_p la L -teoria dei campi di caratteristica p , e sia SCF_p la L -teoria dei campi separabilmente chiusi di caratteristica p . Si noti:

LEMMA 1.2. Se A e B sono campi di caratteristica p , e, posto $L' = L - \{\varepsilon_n\}_{n \geq 0}$, $A \subseteq_{L'} B$, allora $A \subseteq_L B$ se e solo se $\tau(A) = \tau(B)$.

DIMOSTRAZIONE. Sia $\tau(A) = n$, allora $\varepsilon_n^A = 1$ e, se $A \subseteq_L B$, segue $\varepsilon_n^B = 1$, così che $\tau(B) = n$. Se invece $\tau(A) = \infty$, per ogni $n \geq 0$ si ha $\varepsilon_n^B = \varepsilon_n^A = 0$, così che $\tau(B) = \infty$. Viceversa è ovvio che, se $A \subseteq_{L'} B$ e $\tau(A) = \tau(B)$, allora $A \subseteq_L B$.

Il teorema di Eršov si può allora provare sulla base del seguente:

LEMMA 1.3. (1.3.1) SCF_p è model-completa;

(1.3.2) SCF_p è il model-completamento di T_p ;

(1.3.3) Le estensioni complete di SCF_p sono tutte e sole le teorie $SCF_p(n)$ con $0 \leq n < \infty$, dove, se $n < \infty$,

$$SCF_p(n) = SCF_p \cup \{\varepsilon_m = \delta_{mn} : m \geq 0\}$$

mentre

$$SCF_p(\infty) = SCF_p \cup \{\varepsilon_m = 0 : m \geq 0\}.$$

Si confrontino [3], [11] per i dettagli.

Il proposito di questa nota è quello di esporre una classificazione analoga a quella del teorema 1.1 per anelli regolari separabilmente chiusi di caratteristica prima p . La definizione che daremo di anello regolare separabilmente chiuso, utilizzando concetti di teoria dei modelli, è quella di struttura esistenzialmente chiusa per la L -teoria degli anelli regolari. Una caratterizzazione algebrica di tali strut-

ture R sarà comunque presentata nei paragrafi 2 e 3. Tale caratterizzazione algebrica impone a R condizioni meno semplici della primitiva definizione algebrica di campo separabilmente chiuso. Si mostrerà tuttavia come tali condizioni derivino anche da motivazioni essenzialmente algebriche, ad esempio in corrispondenza alla definizione di un concetto di p -dipendenza e di p -base per anelli regolari, o alla connessione con gli anelli regolari differenzialmente chiusi di caratteristica p (si ricordi che ogni campo differenzialmente chiuso di caratteristica p è in particolare un campo separabilmente chiuso con invariante di Eršov ∞).

Si rimanda il lettore a [1] per ogni riferimento di teoria dei modelli, a [4] per l'algebra, a [7] per la topologia e l'algebra booleana.

2. Anelli regolari e p -indipendenza.

Sia R un anello commutativo unitario regolare, cioè tale che in R è definita un'operazione unaria $^{-1}$ (quasi inverso) nel modo seguente: per ogni $a \in R$,

$$a^2 \cdot a^{-1} = a \quad (a^{-1})^2 \cdot a = a^{-1}.$$

OSSERVAZIONE 2.1. Se $\text{car } R = p$, con p primo, e si indica con \mathbf{F}_p il campo con p elementi, allora \mathbf{F}_p è immergibile in R (nel linguaggio $(+, \cdot, -, ^{-1}, 0, 1)$).

OSSERVAZIONE 2.2. Si ha (cfr. [6]) che R è isomorfo all'anello delle sezioni globali $\Gamma(\text{Spec } R, \mathcal{S})$ del fascio di campi di caratteristica p $\mathcal{S} = (R/P : P \in \text{Spec } R)$ sullo spazio booleano $\text{Spec } R$ (dotato della topologia di Zariski, ossia di una base di intorni chiusi e aperti della forma

$$U_e = \{P \in \text{Spec } R : e \notin P\}$$

con e idempotente di R). Si noti a questo proposito che $I(R) = \{e \in R : e^2 = e\}$ è un'algebra di Boole rispetto ad operazioni opportunamente definite (cfr. [7]), ed è isomorfa all'algebra duale di $\text{Spec } R$.

OSSERVAZIONE 2.3. Sia $R^p = \{r^p : r \in R\}$. Evidentemente R^p è sottoanello regolare di R , inoltre si ha

$$R^p = \{r \in R : \forall P \in \text{Spec } R, r + P \in (R/P)^p\},$$

come è agevole dimostrare, poichè l'inclusione \subseteq è ovvia, e l'altra \supseteq si può ottenere, ad esempio, utilizzando la proprietà della partizione per spazi booleani ([6]).

DEFINIZIONE 2.4. Siano R un anello regolare (di caratteristica p), $a_1, \dots, a_n \in R$. Diremo che:

(*) a_1, \dots, a_n sono p -indipendenti su R^p se, per ogni $i = 1, \dots, n$, per ogni $k_i = 0, 1, \dots, p-1$ e per ogni $r_{k_1 \dots k_n} \in R$,

$$\sum_{0 \leq k_i < p} r_{k_1 \dots k_n} a_1^{k_1} \dots a_n^{k_n} = 0$$

implica

$$\prod_{0 \leq k_i < p} (1 - r_{k_1 \dots k_n} (r_{k_1 \dots k_n})^{-1}) \neq 0;$$

(**) a_1, \dots, a_n formano una p -base in R se sono p -indipendenti e, per ogni $b \in R$, a_1, \dots, a_n, b sono p -dipendenti su R^p .

Si noti che la precedente definizione estende i concetti di p -indipendenza e di p -base per insiemi finiti in un campo.

LEMMA 2.5. Siano $a_1, \dots, a_n \in R$ (con R anello regolare di caratteristica p). Allora:

(2.5.1) a_1, \dots, a_n sono p -indipendenti in R se e solo se esiste $P \in \text{Spec } R$ tale che $a_1 + P, \dots, a_n + P$ sono p -indipendenti in R/P ;

(2.5.2) a_1, \dots, a_n sono una p -base per R se e solo se esiste, $P \in \text{Spec } R$ tale che $a_1 + P, \dots, a_n + P$ formano una p -base in R/P e per ogni $P \in \text{Spec } R$, da $a_1 + P, \dots, a_n + P$ è estraibile una p -base per R/P .

DIMOSTRAZIONE. (2.5.1) Supponiamo che, per ogni $P \in \text{Spec } R$, $a_1 + P, \dots, a_n + P$ siano p -dipendenti in R/P , così che esistono $r_{k_1 \dots k_n} \in R$ tali che

$$\sum_{0 \leq k_i < p} r_{k_1 \dots k_n} a_1^{k_1} \dots a_n^{k_n} \in P$$

$$\prod_{0 \leq k_i < p} (1 - r_{k_1 \dots k_n} (r_{k_1 \dots k_n})^{-1}) \in P.$$

Altrettanto vale in un opportuno intorno U_e di P , con $e \in I(R)$. Grazie alla proprietà della partizione degli spazi booleani si può allora defi-

nire $s_{k_1 \dots k_n} \in R$ tale che

$$\sum_{0 \leq k_i < p} s_{k_1 \dots k_n}^p a_1^{k_1} \dots a_n^{k_n} = 0$$

$$\prod_{0 \leq k_i < p} (1 - s_{k_1 \dots k_n} (s_{k_1 \dots k_n})^{-1}) = 0$$

così che, in particolare, a_1, \dots, a_n sono p -dipendenti in R su R^p .

Viceversa, se $\sum_{0 \leq k_i < p} r_{k_1 \dots k_n}^p a_1^{k_1} \dots a_n^{k_n} = 0$ in R , altrettanto vale in R/P , perciò ciascun elemento $r_{k_1 \dots k_n}$ appartiene a P , così che

$$\prod_{0 \leq k_i < p} (1 - r_{k_1 \dots k_n} (r_{k_1 \dots k_n})^{-1}) \notin P;$$

in particolare, il prodotto è diverso da 0 in R .

(2.5.2) Supponiamo che a_1, \dots, a_n formino una p -base per R ; allora a_1, \dots, a_n sono p -indipendenti, ed esiste $P^* \in \text{Spec } R$ tale che $a_1 + P^*, \dots, a_n + P^*$ sono p -indipendenti in R/P^* . Per ogni $b \in R$, poi, a_1, \dots, a_n, b sono p -dipendenti in R , altrettanto sono dunque $a_1 + P, \dots, a_n + P, b + P$ in R/P per ogni $P \in \text{Spec } R$; se quindi $a_1 + P, \dots, a_n + P$ sono p -indipendenti, ad esempio se $P = P^*$, $a_1 + P, \dots, a_n + P$ formano una p -base; in ogni caso, un loro sottoinsieme p -indipendente massimale è una p -base per R/P .

Viceversa, se valgono le ipotesi esposte, a_1, \dots, a_n sono p -indipendenti in R , e, per ogni $b \in R$, a_1, \dots, a_n, b sono p -dipendenti in R , quindi a_1, \dots, a_n formano una p -base per R .

OSSERVAZIONE 2.6. Se a_1, \dots, a_n sono p -indipendenti in R , esiste $P \in \text{Spec } R$ tale che $\tau(R/P) \geq n$; se a_1, \dots, a_n formano una p -base in R , esiste $P \in \text{Spec } R$ tale che $\tau(R/P) = n$ e, per ogni $P \in \text{Spec } R$, $\tau(R/P) \leq n$.

CONTROESEMPIO 2.7. Siano X uno spazio numerabile discreto, $\bar{X} = X \cup \{\infty\}$ la sua compattificazione di Alexandroff. Si ponga, per ogni $x \in \bar{X}$,

$$R_x = \overline{\mathbf{F}_p(t_1)(t_2)} \quad \text{se } x \in X,$$

$$R_\infty = \mathbf{F}_p(t_1)$$

con t_1, t_2 algebricamente indipendenti su \mathbf{F}_p . Definendo in modo ovvio

una topologia su $\bigcup_{x \in \bar{X}} R_x$, si costruisce un fascio $\mathcal{S} = (R_x: x \in \bar{X})$ di campi di caratteristica p sullo spazio booleano \bar{X} ; segue che $R = \Gamma(\bar{X}, \mathcal{S})$ è un anello regolare di caratteristica p , inoltre $\text{Spec } R$ è « naturalmente » omeomorfo a \bar{X} . Inoltre, per ogni $x \in \bar{X}$, R_x ha una p -base finita, anzi $\tau(R_x) = 1$. Tuttavia, R non ammette alcuna p -base finita poichè, per ogni $\sigma \in R$, $\sigma(x) = \sigma(\infty)$ per quasi ogni $x \in X$, quindi $\sigma(x)$ è p -indipendente solo per un numero finito di $x \in X$. Segue che, comunque si fissano $n \geq 1$ e $\sigma_1, \dots, \sigma_n \in R$, l'insieme degli $x \in \bar{X}$ tali che da $\sigma_1(x), \dots, \sigma_n(x)$ è estraibile una p -base per R_x è finito e diverso da \bar{X} . Si noti che, posto $\sigma(x) = t_1$ per ogni $x \in \bar{X}$, si ha: $\sigma \in R$ e l'insieme degli $x \in \bar{X}$ tali che $\sigma(x)$ è p -indipendente si riduce a $\{\infty\}$.

CONTROESEMPIO 2.8. Siano X, \bar{X} come sopra, si ponga, per ogni $x \in \bar{X}$,

$$\begin{aligned} R_x &= \mathbf{F}_p(t_1, t_2) & \text{se } x \in X, \\ R_\infty &= \mathbf{F}_p(t_1) \end{aligned}$$

con t_1, t_2 algebricamente indipendenti su \mathbf{F}_p . Si definisce in modo ovvio un fascio di campi di caratteristica p su \bar{X} , $\mathcal{S} = (R_x: x \in \bar{X})$; $R = \Gamma(\bar{X}, \mathcal{S})$ è un anello regolare di caratteristica p , inoltre $\tau(R_x) = 2$ se $x \in X$, mentre $\tau(R_\infty) = 1$, tuttavia, procedendo come sopra, si deduce che R non ammette alcuna p -base finita.

Si noti che, in questo caso, per ogni $n \geq 1$, e comunque si scelgano $\sigma_1, \dots, \sigma_n$, l'insieme degli $x \in \bar{X}$ tali che $\sigma_1(x), \dots, \sigma_n(x)$ sono p -indipendenti in R_x è aperto e chiuso in \bar{X} ; tuttavia $\{x \in \bar{X}: \tau(R_x) = 1\} = \{\infty\}$.

CONTROESEMPIO 2.9. Sia X uno spazio discreto di cardinalità \aleph_1 , e sia \bar{X} la sua compattificazione di Alexandroff. Si ponga, per ogni $x \in \bar{X}$,

$$\begin{aligned} R_x &= \mathbf{F}_p(S, t) & \text{se } x \in X, \\ R_\infty &= \mathbf{F}_p(S), \end{aligned}$$

dove $|S| = \aleph_0$ e $S \cup \{t\}$ è algebricamente indipendente su \mathbf{F}_p . Si definisce opportunamente un fascio di campi di caratteristica p su \bar{X} $\mathcal{S} = (R_x: x \in \bar{X})$, quindi $R = \Gamma(\bar{X}, \mathcal{S})$ è un anello regolare di carat-

teristica p . Si noti che, per ogni $n \in \mathbf{N} \cup \{\infty\}$,

$$\{x \in \bar{X} : \tau(R_x) = n\} = \begin{cases} \emptyset & \text{se } n \in \mathbf{N}, \\ \bar{X} & \text{se } n = \infty, \end{cases}$$

è comunque aperto e chiuso; e, per ogni $n \geq 1$, qualunque siano $\sigma_1, \dots, \sigma_n \in R$, l'insieme degli $x \in \bar{X}$ tali che $\sigma_1(x), \dots, \sigma_n(x)$ sono p -indipendenti in R_x è anch'esso chiuso e aperto in R_x . Sia comunque $R' \subseteq R$ tale che, per ogni $x \in \bar{X}$, da $\{\sigma(x) : \sigma \in R'\}$ è estraibile una p -base per R_x , ed esiste $x \in \bar{X}$ tale che $\{\sigma(x) : \sigma \in R'\}$ è una p -base per R_x . Poichè, qualunque sia $\sigma \in R$, $\sigma(\infty) = \sigma(x)$ per quasi ogni $x \in \bar{X}$, si deduce da un lato che $|R'| \geq \aleph_1$, dall'altro che $|R'| \leq \aleph_0$ (assurdo).

I controesempi 2.7 e 2.8 giustificano la seguente definizione.

DEFINIZIONE 2.10. Sia R un anello regolare di caratteristica p . Si dice che:

1) R soddisfa (*) se, comunque si fissano $n \geq 1$ ed $a_1, \dots, a_n \in R$, l'insieme degli ideali $P \in \text{Spec } R$ tali che $a_1 + P, \dots, a_n + P$ sono p -indipendenti in R/P è aperto e chiuso in $\text{Spec } R$ (indichiamo con $f_n(a_1, \dots, a_n)$ il corrispondente idempotente);

2) R soddisfa (**) se, per ogni $n \in \mathbf{N}$, $\{P \in \text{Spec } R : \tau(R/P) = n\}$ è un insieme aperto e chiuso (indichiamo con ε_n il corrispondente idempotente).

LEMMA 2.11. Se R è un anello regolare di caratteristica p soddisfacente (*) e (**), R soddisfa anche:

(***) per ogni $n \geq 1$ e comunque si fissano $a_1, \dots, a_n \in R$, l'insieme degli ideali $P \in \text{Spec } R$ per i quali $a_1 + P, \dots, a_n + P$ formano una p -base per R/P è aperto e chiuso.

DIMOSTRAZIONE. Sia $\tau_n(a_1, \dots, a_n) = \varepsilon_n \cdot f_n(a_1, \dots, a_n)$. È facile provare che, se $P \in \text{Spec } R$, allora P appartiene a $U_{\tau_n(a_1, \dots, a_n)}$ se e solo se $a_1 + P, \dots, a_n + P$ formano una p -base in R/P .

Sia R un anello regolare di caratteristica p , verificante (*) e (**). Si hanno tre casi possibili.

CASO A. $\tau(R/P)$ è finito per ogni $P \in \text{Spec } R$. Per (**) e la proprietà della partizione degli spazi booleani, esistono:

1) e_1, \dots, e_m idempotenti di R non nulli, a due a due disgiunti e tali che $\sum_{j=1}^m e_j = 1$,

2) h_1, \dots, h_m interi positivi distinti

tali che, per ogni $j = 1, \dots, m$, se $P \in U_{e_j}$, $\tau(R/P) = h_j$. Per la (*) e ancora per la proprietà della partizione per spazi booleani, per ogni $j = 1, \dots, m$ si possono definire

$$a_{j1}, \dots, a_{jh_j} \in R$$

tali che, per ogni $P \in U_{e_j}$, $a_{j1} + P, \dots, a_{jh_j} + P$ formano una p -base per R/P . Supposto, come è lecito, $h_1 < h_2 < \dots < h_m$, sia, per ogni $j < m$ e per ogni h compreso tra h_{j+1} e h_m , a_{jh} un qualunque elemento di R (ad esempio, sia $a_{jh} = 0$), e si definisca, per ogni $i = 1, \dots, h_m$,

$$a_i = \sum_{j=1}^m e_j a_{ji}.$$

È facile verificare che a_1, \dots, a_{h_m} formano una p -base per R .

CASO B. Esiste $P \in \text{Spec } R$ tale che $\tau(R/P) = \infty$ ma $\{P \in \text{Spec } R: \tau(R/P) = \infty\}$ è un insieme aperto e chiuso U_{e_0} (dove, in particolare, $e_0 \neq 0$). Come sopra, per (***) esistono $e_1, \dots, e_m \in I(R)$ non nulli, disgiunti tra loro e con e_0 , tali che $\sum_{j=0}^m e_j = 1$, ed esistono ancora h_1, \dots, h_m interi positivi distinti per cui, se $j = 1, \dots, m$ e $P \in U_{e_j}$, $\tau(R/P) = h_j$.

Si noti che, in questo caso, può non esistere una p -base per R (nel senso di sottoinsieme R' di R con le proprietà che per ogni $P \in \text{Spec } R$ $\{a + P: a \in R'\}$ contiene una p -base per R/P , ed esiste un ideale $P \in \text{Spec } R$ tale che $\{a + P: a \in R'\}$ è una p -base per R/P : cfr. controesempio 2.9).

CASO C. Esiste $P \in \text{Spec } R$ tale che $\tau(R/P) = \infty$, e $\{P \in \text{Spec } R: \tau(R/P) = \infty\}$ non è un aperto e chiuso di $\text{Spec } R$.

Si noti che $\{P \in \text{Spec } R: \tau(R/P) \neq \infty\}$ coincide con $\bigcup_{n \in \mathbb{N}} \{P \in \text{Spec } R: \tau(R/P) = n\}$ e quindi è un aperto di $\text{Spec } R$, ed ammette un ricoprimento infinito costituito dagli insiemi aperti e chiusi, e non vuoti, della forma $\{P \in \text{Spec } R: \tau(R/P) = n\}$ con $n \in \mathbb{N}$. Anche in questo

caso può non esistere una p -base per R (come si può provare modificando opportunamente il controesempio 2.9).

Sia R un anello regolare di caratteristica p , e consideriamo la seguente condizione:

(\circ) per ogni intero $n > 1$ e per ogni polinomio monico $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in R[x]$ (tale che

$$\prod_{1 \leq i < n} (1 - a_i \cdot a_i^{-1}) = 0$$

se n è potenza di p), esistono due polinomi $g(x) = \sum_{i=0}^{n-1} g_i x^i$ e $h(x) = \sum_{j=0}^{n-1} h_j x^j$ in $R[x]$ tali che

$$f(x) \equiv g(x) \cdot h(x).$$

Si noti che la (\circ) si può esprimere al 1° ordine nel linguaggio dei campi mediante un opportuno insieme infinito di enunciati, e che, se F è un campo di caratteristica p , F soddisfa (\circ) se e solo se F è separabilmente chiuso.

LEMMA 2.13. Se R è un anello regolare di caratteristica p , R soddisfa (\circ) se e solo se, per ogni $P \in \text{Spec } R$, R/P è un campo separabilmente chiuso.

DIMOSTRAZIONE. Analoga ad altre precedentemente svolte.

3. Model-completamento.

Consideriamo allora la classe degli anelli (commutativi unitari) regolari di caratteristica p verificanti (*) e (**). Un linguaggio appropriato per rappresentarla è quello L già adoperato nel § 1 a proposito dei campi. In L consideriamo la teoria RCR_p con i seguenti assiomi:

(a) assiomi di anello commutativo unitario regolare di caratteristica p ;

(b) per ogni $n \geq 1$, gli enunciati:

$$\forall v_1 \dots \forall v_n \quad (f_n(v_1, \dots, v_n) = f_n^2(v_1, \dots, v_n))$$

$$\forall v_1 \dots \forall v_n \quad \forall e \quad (e^2 = e \rightarrow e \cdot f_n(v_1, \dots, v_n) = f_n(ev_1, \dots, ev_n))$$

$$\forall v_1 \dots \forall v_n \quad (f_n(v_1, \dots, v_n) = 0 \leftrightarrow \exists_{0 \leq k_i < p}$$

$$w_{k_1 \dots k_n} \left(\prod_{0 \leq k_i < p} (1 - w_{k_1 \dots k_n} w_{k_1 \dots k_n}^{-1}) = 0 \wedge \sum_{0 \leq k_i < p} w_{k_1 \dots k_n}^p v_1^{k_1} \dots v_n^{k_n} = 0 \right));$$

(c) per ogni $n \in \mathbf{N}$, gli enunciati:

$$\varepsilon_n = \varepsilon_n^2$$

$$\varepsilon_n \varepsilon_m = 0 \quad \text{se } m < n,$$

$$\forall w (f_1(w) \cdot \varepsilon_0 = 0), \quad \exists w (f_1(w) + \varepsilon_0 = 1),$$

$$\forall v_1 \dots \forall v_n \quad \exists w \quad (\varepsilon_n f_n(v_1, \dots, v_n) = 0 \rightarrow \\ \rightarrow f_n(v_1, \dots, v_n)(1 - f_{n+1}(v_1, \dots, v_n, w)) = 0)$$

$$\forall v_1 \dots \forall v_n \quad \forall w \quad (f_n(v_1, \dots, v_n)(1 - f_{n+1}(v_1, \dots, v_n, w)) = \\ = 0 \rightarrow \varepsilon_n f_n(v_1, \dots, v_n) = 0).$$

PROPOSIZIONE 3.1. RCR_p è la L -teoria degli anelli delle sezioni globali di un fascio di campi di caratteristica p su uno spazio booleano. In particolare, se R è modello di RCR_p , R verifica (*) e (**).

DIMOSTRAZIONE. Sia dapprima $R \models RCR_p$, si è già visto come $\text{Spec } R$ sia uno spazio booleano e come la sua algebra duale sia isomorfa ad $I(R)$. Inoltre, per ogni $P \in \text{Spec } R$, R/P è un campo di caratteristica p . Poniamo in R/P , per ogni $n \geq 1$,

$$f_n(r_1 + P, \dots, r_n + P) = f_n(r_1, \dots, r_n) + P,$$

si ha anzitutto:

(3.1.1) f_n è ben definita, ovvero, se è $r_i - r'_i \in P$ per ogni $i = 1, \dots, n$, allora $f_n(r_1, \dots, r_n) - f_n(r'_1, \dots, r'_n) \in P$.

Infatti esiste $e \in I(R)$ tale che $P \in U_e$, e, per ogni $P' \in U_e$, $r_i - r'_i \in P'$ per $i = 1, \dots, n$; in particolare $er_i - er'_i \in P'$ per $i = 1, \dots, n$. D'altra parte, se P' non appartiene ad U_e , allora $e \in P'$ e nuovamente si ha

$er_i - er'_i \in P'$. Segue che $er_i = er'_i$ per ogni $i = 1, \dots, n$, e dunque

$$ef_n(r_1, \dots, r_n) = f_n(er_1, \dots, er_n) = f_n(er'_1, \dots, er'_n) = ef_n(r'_1, \dots, r'_n);$$

poichè $e \notin P$, $f_n(r_1, \dots, r_n) - f_n(r'_1, \dots, r'_n) \in P$.

Notiamo poi:

(3.1.2) $f_n(r_1, \dots, r_n) \in P$ se e solo se esistono $r'_1, \dots, r'_n \in R$ tali che $r_i - r'_i \in P$ per $i = 1, \dots, n$, e $f_n(r'_1, \dots, r'_n) = 0$.

L'implicazione \leftarrow è ovvia. Riguardo a \rightarrow , posto $f = 1 - f_n(r_1, \dots, r_n)$, si ha:

$$0 = f_n(r_1, \dots, r_n)f = f_n(fr_1, \dots, fr_n)$$

$$r_i - fr_i = r_i f_n(r_1, \dots, r_n) \in P.$$

Segue che

$$\begin{aligned} \{(r_1 + P, \dots, r_n + P): f_n(r_1 + P, \dots, r_n + P) = P\} = \\ = \{(r_1 + P, \dots, r_n + P): f_n(r_1, \dots, r_n) = 0\}. \end{aligned}$$

(3.1.3) La struttura $(R/P; +, \cdot, -, ^{-1}, (f_n)_{n \geq 1}; 0, 1, (\varepsilon_n + P)_{n \geq 0})$ verifica gli enunciati di cui ai punti (b) e (c).

Sia ora \mathcal{S} l'unione disgiunta $\bigcup_P R/P$ (al variare di P in $\text{Spec } R$), e su \mathcal{S} consideriamo la topologia che ammette come base di aperti per ogni punto $r + P$ la famiglia $\{\mathcal{S}(r, e): e \in I(R), P \in U_e\}$, dove $\mathcal{S}(r, e) = \{r + P': P' \in U_e\}$.

$\mathcal{S} = (R/P: P \in \text{Spec } R)$ è allora un fascio di campi in L , in particolare, per ogni $n \geq 1$, $r_1, \dots, r_n \in R$,

$$\{P \in \text{Spec } R: f_n(r_1 + P, \dots, r_n + P) = 1 + P\}$$

è un insieme aperto e chiuso di $\text{Spec } R$ e coincide con

$$U_{f_n(r_1, \dots, r_n)},$$

e, per ogni $n \in \mathbb{N}$, $\{P \in \text{Spec } R: \tau(R/P) = \underline{n}\}$ è un insieme aperto e chiuso

di $\text{Spec } R$, e coincide anzi con U_{ε_n} : di conseguenza R soddisfa (*) e (**).

L'anello $\Gamma(\text{Spec } R, \mathbb{S})$ delle sezioni globali di \mathbb{S} su $\text{Spec } R$ è una L -sottostruttura di $\prod_P R/P$, ed è isomorfo (come anello) a R , d'altra parte, ricordando la definizione di f_n e di ε_n in R/P , è facile verificare che tale isomorfismo rispetta anche gli ulteriori simboli di L .

Viceversa, se $\mathbb{S} = (R_x: x \in X)$ è un L -fascio di campi di caratteristica p su uno spazio booleano X , e $\Gamma(X, \mathbb{S})$ è il relativo anello delle sezioni globali, considerato come L -sottostruttura di $\prod_{x \in X} R_x$, si ha anzitutto che $\Gamma(X, \mathbb{S})$ è un anello regolare di caratteristica p , e si può comunque verificare che $\Gamma(X, \mathbb{S})$ soddisfa gli ulteriori assiomi (quelli relativi ai gruppi (b) e (c)) di RCR_p .

Sia RCR_p^* la teoria che si ottiene aggiungendo a RCR_p i seguenti assiomi:

(d) gli enunciati corrispondenti alla proprietà (o);

(e) l'enunciato che assicura che R non ammette idempotenti minimali (cioè $I(R)$ è priva di atomi, cioè $\text{Spec } R$ è privo di punti isolati: a questo proposito, diremo spazio cantoriano ogni spazio booleano privo di punti isolati).

PROPOSIZIONE 3.2. RCR_p^* è la L -teoria degli anelli delle sezioni globali di un fascio di campi separabilmente chiusi di caratteristica p su uno spazio cantoriano.

DIMOSTRAZIONE. Segue dalla proposizione 3.1 e dal lemma 2.13.

TEOREMA 3.3. RCR_p^* è il model-completamento di RCR_p .

DIMOSTRAZIONE. Segue da [9], teorema 4.10 (vi) e corollario 4.11. oltre che dal precedente lemma 1.3.

Osserviamo che tanto RCR_p^* quanto RCR_p sono teorie di Horn, e quindi si conservano per prodotti diretti.

OSSERVAZIONE 3.4. In [5] si trova un analogo del teorema degli zeri di Hilbert, valido per campi separabilmente chiusi, il quale, da un punto di vista algebrico, può così essere formulato:

« se A e B sono campi di caratteristica p , $A, B \models SCF_p$ e $A \subset_L B$ (così che $\tau(A) = \tau(B)$ ed A è estensione p -basica di B), ogni sistema finito di equazioni a coefficienti in A ammette soluzione in A se e solo se ammette soluzione in B ».

Un risultato analogo per anelli regolari, modelli di RCE_p^* (e quindi separabilmente chiusi nel senso del teorema 3.3), è ovviamente assicurato dal fatto che RCE_p^* è model-completa, così che, se $R, S \models RCE_p^*$ e $R \subseteq_L S$, allora $R <_1 S$, e dunque ogni sistema finito di equazioni a coefficienti in R ha soluzione in R se e solo se ha soluzione in S .

4. Estensioni complete.

RCE_p^* non è evidentemente completa; per individuarne le estensioni complete, consideriamo l'insieme $P(\mathbb{N})$ delle parti di \mathbb{N} , e per ogni $M \in P(\mathbb{N})$, definiamo

$$q(M) = \{\varepsilon_m \neq 0 : m \in M\} \cup \{\varepsilon_m = 0 : m \notin M\}$$

e, se M è finito e non vuoto,

$$q_0(M) = q(M) \cup \left\{ \sum_{m \in M} \varepsilon_m = 1 \right\},$$

$$q_1(M) = q(M) \cup \left\{ \sum_{m \in M} \varepsilon_m \neq 1 \right\}.$$

TEOREMA 4.1. Sia $M \in P(\mathbb{N})$.

(4.1.1) Se M è finito e non vuoto, $RCE_p^* \cup q_0(M)$ è completa;

(4.1.2) se M è finito e non vuoto, $RCE_p^* \cup q_1(M)$ è completa;

(4.1.3) se M è infinito, oppure $M = \emptyset$, $RCE_p^* \cup q(M)$ è completa;

(4.1.4) non esistono altre estensioni complete di RCE_p^* .

DIMOSTRAZIONE. Per ogni $n \in \mathbb{N} \cup \{\infty\}$, la teoria completa $SCF_p(n)$ ammette un modello ω_1 -saturato, che indichiamo con A_n , e nel quale è immergibile ogni modello numerabile di $SCF_p(n)$.

(4.1.1) $RCE_p^* \cup q_0(M)$ è model-completa, così che, per ottenere la completezza, basta provare che, ad esempio, essa gode della J.E.P., ovvero che, per ogni coppia di modelli di $RCE_p^* \cup q_0(M)$ (che non è restrittivo supporre numerabili a causa del teorema di Löwenheim-Skolem), esiste un terzo modello nel quale sono entrambi (elementar-

mente) immergibili. Sia dunque $R \models RCR_p^* \cup q_0(M)$, $|R| = \aleph_0$, allora $R \simeq_L \Gamma(\text{Spec } R, \mathcal{S})$, dove $\text{Spec } R$ è omeomorfo allo spazio di Cantor 2^ω , e \mathcal{S} è il fascio di campi $(R/P: P \in \text{Spec } R)$. Inoltre, posto $M = \{m_1, \dots, m_s\}$ e $U_j = U_{\varepsilon_{m_j}}$ per $j = 1, \dots, s$, si ha:

- 1) $\text{Spec } R = \bigcup_{j=1}^s U_j$,
- 2) $U_j \neq \emptyset$ per ogni $j = 1, \dots, s$,
- 3) se $P \in U_j$, allora $\tau(R/P) = m_j$.

Si ha:

$$R \simeq \Gamma(\text{Spec } R, \mathcal{S}) \subseteq \prod_P R/P \subseteq \prod_{j=1}^s A_{m_j}^c \subseteq \prod_{j=1}^s C^0(2^\omega, A_{m_j})^c$$

dove $c = 2^{\aleph_0}$, così che $\prod_{j=1}^s C^0(2^\omega, A_{m_j})^c$ non dipende da R , ed è modello di $RCR_p^* \cup q_0(M)$ (in particolare, è modello di RCR_p^* poichè ciascun $C^0(2^\omega, A_{m_j})^c$ è modello di RCR_p^* , e RCR_p^* è una teoria di Horn).

(4.1.2) $RCR_p^* \cup q_1(M)$ è model-completa, come sopra basta dunque provare che ha la J.E.P. Sia dunque R modello numerabile di $RCR_p^* \cup q_1(M)$, allora R è L -isomorfo a $\Gamma(\text{Spec } R, \mathcal{S})$, dove $\text{Spec } R$ è omeomorfo allo spazio di Cantor 2^ω e \mathcal{S} è il fascio di L -campi $(R/P: P \in \text{Spec } R)$. Posto $M = \{m_1, \dots, m_s\}$ e $m_0 = \infty$, $U_j = U_{\varepsilon_{m_j}}$ se $j = 1, \dots, s$, $U_0 = C\left(\bigcup_{j=1}^s U_j\right)$, si ha:

- 1) $U_j \neq \emptyset$ per ogni $j = 0, 1, \dots, s$;
- 2) se $P \in U_j$, $\tau(R/P) = m_j$ per $j = 0, 1, \dots, s$.

Si ha dunque

$$R \simeq \Gamma(\text{Spec } R, \mathcal{S}) \subseteq \prod_P R/P \subseteq \prod_{j=1}^s A_{m_j}^c \subseteq \prod_{j=1}^s C^0(2^\omega, A_{m_j})^c$$

dove $c = 2^{\aleph_0}$, $\prod_{j=1}^s C^0(2^\omega, A_{m_j})^c$ non dipende da R , ed è modello di $RCR_p^* \cup q_1(M)$.

(4.1.3) Se $M = \emptyset$, si procede come in (4.1.2). Se M è infinito, $RCR_p^* \cup q(M)$ è model-completa, così che basta provare che ha la

J.E.P.; sia dunque R un modello numerabile di $R\mathcal{C}R_p^* \cup q(M)$, allora $\text{Spec } R$ è omeomorfo a 2^ω , e, posto $U_m = U_{\varepsilon_m}$ per ogni $m \in M$ e $U = \mathcal{C}\left(\bigcup_{m \in M} U_m\right)$, si ha che U_m è chiuso, aperto e non vuoto, mentre U è chiuso ma non aperto in $\text{Spec } R$; inoltre, se $P \in U_m$, $\tau(R/P) = m$, mentre, se $P \in U$, $\tau(R/P) = \infty$. Si ha:

$$R \simeq \Gamma(\text{Spec } R, \mathcal{S}) \subseteq \prod_P R/P \subseteq \prod_{m \in M \cup \{\infty\}} A_m^c \subseteq \prod_{m \in M \cup \{\infty\}} \mathcal{C}^0(2^\omega, A_m)^c$$

che, al solito, non dipende da R , ed è modello di $R\mathcal{C}R_p^*$, oltre a soddisfare $q(M)$.

(4.1.4) È ovvio. Si noti che $R\mathcal{C}R_p^*$ ha 2^{\aleph_1} estensioni complete.

OSSERVAZIONE 4.2. Se $M = \emptyset$, R è modello di $R\mathcal{C}R_p^* \cup q(M)$ se e solo se $R \models R\mathcal{C}R_p^*$ e, per ogni $P \in \text{Spec } R$, $\tau(R/P) = \infty$, ovvero se e solo se R è l'anello delle sezioni globali di un L -fascio di modelli di $\mathcal{S}\mathcal{C}\mathcal{F}_p(\infty)$ su uno spazio cantoriano.

OSSERVAZIONE 4.3. Se $M = \{m\}$, R è modello di $R\mathcal{C}R_p^* \cup q_0(M)$ se e solo se $R \models R\mathcal{C}R_p^*$ e, per ogni $P \in \text{Spec } R$, $\tau(R/P) = m$, ovvero se e solo se R è l'anello delle sezioni globali di un L -fascio di modelli di $\mathcal{S}\mathcal{C}\mathcal{F}_p(m)$ su uno spazio cantoriano.

OSSERVAZIONE 4.4. Si noti che, per ogni modello di $R\mathcal{C}R_p$, ciascun simbolo f_n, ε_n è definibile a partire dagli altri simboli di L , di modo che ogni estensione completa di $R\mathcal{C}R_p^*$ rimane tale anche nel linguaggio degli anelli commutativi unitari regolari.

OSSERVAZIONE 4.5. Nessuna estensione completa di $R\mathcal{C}R_p^*$ è stabile, poichè, per ogni $R \models R\mathcal{C}R_p^*$, l'algebra di Boole $I(R)$ è definibile in R , e priva di atomi, quindi instabile.

Circa i modelli di $R\mathcal{C}R_p$ che sono stabili e/o \aleph_1 -categorici, possiamo comunque affermare:

PROPOSIZIONE 4.6. Sia $R \models R\mathcal{C}R_p$. Allora:

(4.6.1) R è ω -stabile se e solo se è superstabile, se e solo se $\text{Spec } R$ è finito e, per ogni $P \in \text{Spec } R$, R/P è un campo finito o algebricamente chiuso;

(4.6.2) R è \aleph_1 -categorico se e solo se R è ω -stabile ed esiste al più un $P \in \text{Spec } R$ tale che R/P è un campo algebricamente chiuso;

(4.6.3) se $\text{Spec } R$ è finito e, per ogni $P \in \text{Spec } R$, $R/P \models SCF_p$, R è stabile.

Considerando che f_n, ε_n sono definibili in R , la proposizione 4.6 è implicita nella letteratura esistente sulla stabilità: si vedano comunque [2], e, limitatamente a (4.6.3), [11]. La (4.6.3) dà esempi di modelli di RCR_p stabili ma non superstabili.

OSSEVAZIONE 4.7. In [8] è data una definizione di anello regolare differenzialmente chiuso (di caratteristica p); senza richiamarla qui nei dettagli, notiamo comunque che essa estende naturalmente, anche da un punto di vista algebrico, la nozione di campo differenzialmente chiuso di caratteristica p ([10]). Indichiamo allora con RDR_p^* la teoria degli anelli commutativi unitari regolari differenzialmente chiusi di caratteristica p , e sia $R \models RDR_p^*$. Allora $\text{Spec } R$ è uno spazio cantoriano e, per ogni $P \in \text{Spec } R$, R/P è un campo differenzialmente chiuso di caratteristica p , e quindi è un campo separabilmente chiuso, anzi, siccome R/P ha dimensione lineare infinita sul suo campo costante, $R/P \models SCF_p(\infty)$. In particolare, R soddisfa la condizione (o). Si definisca poi il wronskiano $w_n(v_1, \dots, v_n)$ nel modo consueto come il determinante

$$w_n(v_1, \dots, v_n) = \begin{vmatrix} v_1 & v_2 & \cdots & v_n \\ Dv_1 & Dv_2 & \cdots & Dv_n \\ \cdots & \cdots & \cdots & \cdots \\ D^{n-1}v_1 & D^{n-1}v_2 & \cdots & D^{n-1}v_n \end{vmatrix}$$

(dove D indica l'operazione di derivazione in R), e sia $w'_n(v_1, \dots, v_n)$ il determinante wronskiano della matrice di ordine p^n la cui prima riga si compone di tutti i possibili prodotti della forma

$$v_1^{k_1} \dots v_n^{k_n}$$

con $0 \leq k_i < p$ per $i = 1, \dots, n$; sia finalmente

$$f_n(v_1, \dots, v_n) = w'_n(v_1, \dots, v_n)(w_n(v_1, \dots, v_n))^{-1}.$$

Allora $f_n(v_1, \dots, v_n)$ è idempotente e, per ogni $e \in I(R)$, si ha

$$f_n(ev_1, \dots, ev_n) = ef_n(v_1, \dots, v_n)$$

dato che

$$w'_n(ev_1, \dots, ev_n) = e^{pn}w'_n(v_1, \dots, v_n) = ew'_n(v_1, \dots, v_n).$$

Infine si ha $f_n(v_1, \dots, v_n) = 0$ se e solo se $w'_n(v_1, \dots, v_n) = 0$, ovvero $w'_n(v_1 + P, \dots, v_n + P) = P$ per ogni $P \in \text{Spec } R$. Di conseguenza in R/P gli elementi

$$v_1^{k_1} \dots v_n^{k_n} + P$$

(con $0 \leq k_i < p$ per $i = 1, \dots, n$) sono linearmente dipendenti sul sottocampo costante, ovvero su $(R/P)^p$ dato che R/P è differenzialmente chiuso e quindi differenzialmente perfetto; quindi $v_1 + P, \dots, v_n + P$ sono p -dipendenti in R/P per ogni $P \in \text{Spec } R$, così che, finalmente, v_1, \dots, v_n sono p -dipendenti in R (cfr. Lemma 2.5.1). Si può dedurre che in R $f_n(v_1, \dots, v_n) = 0$ se e solo se v_1, \dots, v_n sono p -dipendenti.

Ponendo infine $\varepsilon_n = 0$ per ogni $n \in \mathbb{N}$, si verifica che R è modello della teoria completa $RCR_p^* \cup q(\emptyset)$, che, come già notato, è la corrispondente per anelli regolari della teoria $SCF_p(\infty)$.

BIBLIOGRAFIA

- [1] G. CHERLIN, *Model-theoretic algebra. Selected topics*, Lecture Notes in Mathematics 521, Springer, 1975.
- [2] G. CHERLIN - J. REINEKE, *Categoricity and stability of commutative rings*, Ann. Math. Logic, **10** (1976), pp. 367-399.
- [3] Y. ERSOV, *Fields with a solvable theory*, Dokl. Akad. Nauk SSSR, **174** (1967), pp. 19-20; traduzione inglese in Sov. Math., **8** (1967), pp. 575-576.
- [4] N. JACOBSON, *Lectures in abstract algebra*, vol. III, Van Nostrand, 1964.
- [5] S. LANG, *Introduction to algebraic geometry*, Addison-Wesley, 1958.
- [6] R. S. PIERCE, *Modules over commutative regular rings*, Mem. Amer. Math. Soc., **70**, 1967.
- [7] D. PONASSE - J. C. CARREGA, *Algèbre et topologie booléennes*, Masson, 1979.
- [8] C. TOFFALORI, *Strutture differenzialmente chiuse per alcune classi di anelli*, in corso di stampa.
- [9] V. WEISPFENNING, *Model-completeness and elimination of quantifiers for subdirect products of structures*, J. Algebra, **36** (1975), pp. 252-277.

- [10] C. WOOD, *Notes on the stability of separably closed fields*, J. Symbolic Logic, **44** (1979), pp. 412-416.
- [11] C. WOOD, *The model theory of differential fields revisited*, Israel J. Math., **25** (1976), pp. 331-352.

Manoscritto pervenuto in redazione il 5 Maggio 1982