Dal teorema 22 segue infatti che la totalità dei sotto-corpi di K separabili sopra k genera un massimo corpo K_0 separabile sopra k. Se, nel caso $K_0 \neq K$, il corpo K non fosse puramente inseparabile sopra K_0 allora potrebbe facilmente trovarsi un elemento $x \subset\!| K_0$ tale che (K_0, x) fosse separabile sopra K_0 e dunque (ved. 21) separabile anche sopra k.

§ 3. Dipendenza lineare di differenziali e dipendenza algebrica di elementi.

Il noto legame fra la dipendenza analitica di funzioni e la dipendenza lineare dei loro differenziali totali ritrovasi pure partendo dal nostro punto di vista algebrico.

27. *Se in un corpo algebrico e separabile su k sono linearmente indipendenti i differenziali relativi* $\frac{d}{k}x_1, \frac{d}{k}x_2, \dots, \frac{d}{k}x_m$ $(x_i \in K)$, *allora sono algebricamente indipendenti sopra k gli elementi* $x_1, x_2, \dots, x_m$.

DIMOSTRAZIONE. - Essendo il corpo $(k, x_1, \dots, x_m) = K_0$ separabile sopra k (teorema 20) avremo $\dim \frac{K_0}{k} = \text{rango } K_0 \cdot \frac{d_0}{k} K_0$, da cui, tenuto conto che $m \geq \text{rango } K_0 \cdot \frac{d_0}{k} K_0 \geq \text{rango } K \cdot \frac{d}{k} K_0 = m$, segue $\dim \frac{K_0}{k} = m$, c. d. d.

28. *Se in un corpo K algebrico, separabile e n-dimensionale sopra k sono linearmente indipendenti i differenziali relativi* $\frac{d}{k}x_1, \frac{d}{k}x_2, \dots, \frac{d}{k}x_n$, *esso è separabile e 0-dimensionale su* $(k, x_1, x_2, \dots, x_n)$.

DIMOSTRAZIONE. - Si osservi dapprima che $(k, x_1, \dots, x_n) = K_0$ è n-dimensionale su k (ved. 27). Designando y un elemento qualunque di K, il corpo $(k, x_1, \dots, x_n, y) = K_1$ è separabile sopra k (teorema 20). Se dunque $f(x_1, \dots, x_n, y) = 0$ definisce K_1 sopra K_0, nella relazione

$$f_y \cdot \frac{d_1}{k} y + \sum_{i=1}^{n} f_{x_i} \cdot \frac{d_1}{k} x_i = 0,$$

che definisce il modulo

$$K_1 \cdot \frac{d_1}{k} K_1 = K_1 \cdot \frac{d_1}{k} y + \sum_{i=1}^{n} K_1 \cdot \frac{d_1}{k} x_i,$$

non possono essere zero tutte le $n+1$ derivate parziali. Se fosse $f_y = 0$, si otterrebbe da quella relazione una dipendenza lineare fra i differenziali $\frac{d_1}{k} x_i$ che varrebbe anche per i $\frac{d}{k} x$. Ne segue $f_y \neq 0$, il che esprime la separabilità di $(k, x_1, \dots, x_n, y)$ sopra K_0. Dal teorema 22 risulta che K, potendo esso generarsi sopra K_0 mediante un numero finito di tali corpi $(k, x_1, \ldots, x_n, y)$, è separabile sopra il corpo n-dimensionale K_0. C. d. d.

29 È noto il teorema dell'esistenza di un elemento primitivo:

Se in un corpo $(k, x_1, \ldots, x_m)$, 0-dimensionale su k, sono separabili sopra k i corpi (k, x_i), $(i = 1, 2, \ldots, m-1)$, esiste un elemento z tale che $(k, x_1, \ldots, x_m) = (k, z)$.

Ne segue immediatamente:

30. *Sotto le ipotesi del teorema* **28** *esiste un elemento y tale che $K = (k, x_1, \ldots, x_n, y)$ sia definito da $f(x_1, \ldots, x_n, y) = 0$, con $f_y \neq 0$.*

31. *Nel caso di un corpo K algebrico sopra k di caratteristica 0 la dipendenza lineare di differenziali relativi a k corrisponde precisamente alla dipendenza algebrica sopra k degli elementi differenziati.*

DIMOSTRAZIONE. - Per il teorema **27** basta dimostrare la indipendenza lineare dei differenziali $\frac{d}{k}x_1, \ldots, \frac{d}{k}x_m$ di elementi $x_1, \ldots, x_m$ algebricamente indipendenti.

Possiamo sempre assumere che $x_1, \ldots, x_m$ siano contenuti in un sistema $x_1, \ldots, x_n$ di n elementi algebricamente indipendenti su k, designando con n la dimensione di K sopra k. Dal teorema **29** segue allora che si ha $K = (k, x_1 \ldots, x_n, y)$ con

$$f_y \cdot \frac{d}{k} y + \sum_{i=1}^{n} f_{x_i} \cdot \frac{d}{k} x_i = 0, \quad f_y \neq 0.$$

Essendo

$$K \cdot \frac{d}{k} K = K \cdot \frac{d}{k} y + \sum_{i=1}^{n} K \cdot \frac{d}{k} x_i, \qquad \text{rango } K \cdot \frac{d}{k} K = \dim \frac{K}{k} = n,$$

è chiaro ormai che i differenziali $\frac{d}{k} x_i$ $(i = 1, \ldots, m)$ debbono essere linearmente indipendenti. C. d. d.

32. Ricordiamo la definizione: Un corpo k è chiamato p e r f e t t o se, essendo $p \neq 0$ la sua caratteristica, l'insieme k^p delle p-esime potenze degli elementi di k coincide con k oppure se la sua caratteristica è 0.

Ogni corpo K algebrico su un corpo perfetto k è separabile sopra k.

DIMOSTRAZIONE. - Basta considerare il caso di caratteristica $p \neq 0$.

Poichè in questo caso è supposto ogni elemento a di k essere della forma $a = b^p$, si ha $da = pb^{p-1} \cdot db = 0$ cosicchè la differenziazione assoluta di K coincide con quella di K sopra k.

Siano $x_1, x_2, \ldots, x_m$ elementi di K algebricamente dipendenti sopra k e $f(x_1, x_2, \ldots, x_m) = 0$ una relazione di grado minimo. Nell'equazione differenziale $\sum_{i=1}^{m} f_{x_i} \cdot dx_i = 0$ non possono essere zero tutti i coefficienti f_{x_i}:

nè identicamente,

perché allora $f(x_1, x_2, \ldots, x_m) = 0$ sarebbe della forma

$$\Sigma\, a_{n_1 n_2 \ldots n_m} \cdot x_1^{pn_1} \cdot x_2^{pn_2} \cdot \ldots \cdot x_m^{pn_m} = 0$$

oppure, essendo $a_{n_1 n_2 \ldots n_m} = b^p_{n_1 n_2 \ldots n_m}$ con $b_{n_1 n_2 \ldots n_m} \in k$, della forma

$$(\Sigma\, b_{n_1 n_2 \ldots n_m} \cdot x_1^{n_1} \cdot x_2^{n_2} \ldots x_m^{n_m})^p = 0,$$

che condurrebbe ad una relazione

$$\Sigma\, b_{n_1 n_2 \ldots n_m} \cdot x_1^{n_1} \cdot x_2^{n_2} \ldots x_m^{n_m} = 0$$

di grado minore di quello di $f = 0$,

nè in altro modo,

perché in tal caso una almeno delle equazioni $f_{x_i} = 0$ costituirebbe altresì una relazione di grado minore di quello di $f = 0$.

Da ciò risulta che $dx_1, dx_2, \ldots, dx_m$ sono linearmente dipendenti.

Ora, se K è n-dimensionale sopra k, $n+1$ elementi di K sono sempre algebricamente dipendenti sopra k. Non esistendo dunque in K più che n differenziali assoluti (= relativi) linearmente indipendenti, è chiaro ormai che K è separabile sopra k. C. d. d.

33. Poiché il corpo primo di un corpo K, cioè il sottocorpo (1) di K generato dall'elemento 1 di K, è sempre perfetto, e poiché i corpi aritmetici possono definirsi anche quali corpi algebrici sopra il loro corpo primo, possiamo, in conseguenza del teorema **30** e della dimostrazione **32**, constatare:

In un corpo aritmetico K segue sempre dalla dipendenza algebrica di elementi di K la dipendenza lineare dei loro differenziali. Se $\dim K = n$, $K \cdot dK = K \cdot dx_1 + \ldots + K \cdot dx_n$, esiste un elemento y di K tale che $K = (x_1, \ldots, x_n, y)$ sia definito da $f(x_1, \ldots, x_n, y) = 0$ con $f_y \neq 0$.

34. Nel caso in cui la caratteristica sia $p \neq 0$, non c'è da aspettarsi un'analogia diretta col teorema **31**, dato che è zero il differenziale di ogni p-esima potenza x^p $(x \in K)$. Però si ottiene un'analogia indiretta intercalando il corpo K^p costituito dalle p-esime potenze di tutti gli elementi di K. Il fatto che questo insieme K^p è un corpo, risulta dalle identità $(x+y)^p = x^p + y^p$, $(x \cdot y)^p = x^p \cdot y^p$ che mostrano inoltre che con $x \to x^p$ $(x \in K)$ è definito un isomorfismo di K su K^p.

Per stabilire quell'analogia annunciata, dimostriamo dapprima:

35. *Se per un corpo K, algebrico e puramente inseparabile su k, vale* $K \cdot \frac{d}{k} K = \sum_{i=1}^{m} K \cdot \frac{d}{k} x_i$, *il corpo K può generarsi nel modo seguente* $K = (k, x_1, x_2, \ldots, x_m)$.

DIMOSTRAZIONE. - Ponendo $(k, x_1, x_2, \ldots, x_m) = K_0$ si deduce dall'ipotesi del teorema

$$K \cdot \frac{d}{K_0} K = \sum_{i=1}^{m} K \cdot \frac{d}{K_0} x_i = 0$$

il che esprime K essere 0-dimensionale e separabile su K_0. Secondo il teorema 30 vale dunque $K = (K_0, y)$. Ma essendo K puramente inseparabile sopra k, l'elemento y soddisfa ad un'equazione $y^{p^\lambda} - a = 0$ con $a \in k \subset K_0$. L'osservazione 24 mostra allora $y \subset K_0$ cioè $K = K_0$, perchè altrimenti K sarebbe inseparabile sopra K_0. C. d. d.

36. *Nel caso in cui K sia di caratteristica $p \neq 0$ e algebrico sopra k, le due affermazioni*

$$\frac{d}{k} z \subset K \cdot \frac{d}{k} x_1 + \ldots + K \cdot \frac{d}{k} x_m \quad \text{e} \quad z \subset (k, K^p, x_1, x_2, \ldots, x_m)$$

sono equivalenti.

DIMOSTRAZIONE. - I. Da $z \subset (k, K^p, x_1, x_2, \ldots, x_m)$ segue

$$\frac{d}{k} z \subset K \cdot \frac{d}{k} K^p + \sum_{i=1}^{m} K \cdot \frac{d}{k} x_i \text{ e perciò } \frac{d}{k} z \subset \sum_{i=1}^{m} K \cdot \frac{d}{k} x_i,$$

essendo $dx^p = 0$ per x qualunque di K.

II. Viceversa, supponiamo

$$(*) \qquad \frac{d}{k} z = \sum_{i=1}^{m} a_i \cdot \frac{d}{k} x_i \qquad (a_i \in K).$$

Possiamo limitarci al caso in cui i differenziali $\frac{d}{k} x_i$ siano linearmente indipendenti.

Il corpo K, algebrico su k, è algebrico e anche puramente inseparabile su $K_0 = (k, K^p)$ poichè per x qualunque di K vale $x^p \subset K_0$.

Se supponiamo dunque

$$(**) \qquad K \cdot \frac{d}{K_0} K = \sum_{i=1}^{n} K \cdot \frac{d}{K_0} z_i, \quad \left(n = \text{rango } K \cdot \frac{d}{K_0} K\right)$$

il teorema precedente mostra che $K = (K_0, z_1, z_2, \ldots, z_n)$.

Ponendo $(K_0, z_1, z_2, \dots, z_h) = K_h$, $(0 \leq h \leq n)$, avremo

$$(_*{}^*{}_*) \qquad K_h = K_{h-1} + K_{h-1} \cdot z_h + \dots + K_{h-1} \cdot z_h^{p-1}$$

(il che significa che ogni elemento di K_h è combinazione lineare di $1, z_h, \dots, z_h^{p-1}$ con coefficienti appartenenti a K_{h-1}), essendo

$$(^\circ) \qquad z_h^p - a_h = 0 \quad \text{con} \quad a_h \in K_0 \subset K_{h-1}.$$

L'applicazione successiva delle $(_*{}^*{}_*)$ conduce alla conclusione

$$(^{\circ\circ}) \qquad K = \sum_{0 \leq m_i < p} K_0 \cdot z_1^{m_1} z_2^{m_2} \dots z_n^{m_n}.$$

Supposto che valga una relazione

$$({}_\circ{}^\circ{}_\circ) \qquad \sum_{0 \leq m_i < p} a_{m_1 m_2 \dots m_n} \cdot z_1^{m_1} z_2^{m_2} \dots z_n^{m_n} = 0 \quad \text{con} \quad a_{m_1 m_2 \dots m_n} \in K_0$$

senza che siano zero tutti i coefficienti $a_{m_1 m_2 \dots m_n}$, scegliamo $h \leq n$ tale che nella $({}_\circ{}^\circ{}_\circ)$ non siano effettivamente presenti le z_l con $l > h$ mentre vi sia presente la z_h. Allora la $({}_\circ{}^\circ{}_\circ)$ esprimerebbe che z_h soddisfa rispetto *a* K_{h-1}, ad un'equazione di grado minore di p cosicchè l'equazione $(^\circ)$ sarebbe riducibile e pertanto (ved. 24) $z_h \subset K_{h-1}$. L'elemento z_h sarebbe dunque superfluo nel generare il corpo K: $(K_0, z_1, \dots, z_{h-1}, z_{h+1}, \dots, z_n)$ e si avrebbe

$$\text{rango } K \cdot \frac{d}{K_0} K \leq n - 1$$

contro l'ipotesi $(**)$.

Avendo dimostrato che la $({}_\circ{}^\circ{}_\circ)$ è possibile solamente se tutti i coefficienti $a_{m_1 m_2 \dots m_n}$ sono zero, se ne conclude che nell'espressione

$$(+) \qquad z = \sum_{0 \leq m_i < p} c_{m_1 m_2 \dots m_n} \cdot z_1^{m_1} \cdot z_2^{m_2} \dots z_n^{m_n}, \quad (c_{m_1 m_2 \dots m_n} \in K_0)$$

con cui, secondo $(^{\circ\circ})$, può scriversi l'elemento z considerato nell'ipotesi $(*)$, i coefficienti $c_{m_1 m_2 \dots m_n}$ sono determinati univocamente da z.

Ora è chiaro che la differenziazione di K rispetto a k coincide con quella di K rispetto a $K_0 = (k, K^p)$, dato che i differenziali degli elementi di K^p sono automaticamente zero. L'ipotesi che i differenziali

$$(++) \qquad \frac{d}{k} x_i = \frac{d}{K_0} x_i \qquad (i = 1, 2, \dots, m)$$

siano linearmente indipendenti ci permette di supporre in $(**)$ $z_i = x_i$ per $i = 1, 2, \dots, m$.

Dalla $(+)$ segue

$$\frac{d}{K_0} z = \sum_{i=1}^{n} \Big(\sum_{0 \leq m_\nu < p} m_i c_{m_1 \dots m_i \dots m_n} \cdot z_1^{m_1} \dots z_i^{m_i - 1} \dots z_n^{m_n} \Big) \cdot \frac{d}{K_0} z_i.$$

Tenendo conto di (*), (++) e della indipendenza lineare dei $\frac{d}{K_0} z_i$ $(i = 1, 2, \ldots, m)$ se ne deducono le relazioni

$$\sum_{0 \le m_\nu < p} m_i c_{m_1 \ldots m_i \ldots m_n} \cdot z_1^{m_1} \ldots z_i^{m_i - 1} \ldots z_n^{m_n} = 0 \quad \text{per} \quad i > m$$

che alla loro volta dànno $m_i c_{m_1 \ldots m_i \ldots m_n} = 0$ per $i > m$, dimostrando così (si osservi che $m_i < p =$ caratteristica di K) che in (+) non entrano effettivamente che gli elementi $z_i = x_i$ $(i \le m)$.

Ma ciò è proprio quello che volevasi dimostrare.

37. *Se un corpo K è algebrico su k con $\dim \frac{K}{k} = n$ e inseparabilità relativa $i > 0$, esso può generarsi su k con $n + i$, ma non con meno elementi.*

DIMOSTRAZIONE. - I. Sia

$$(*) \qquad K \cdot \frac{d}{k} K = \sum_{h=1}^{n+i} K \cdot \frac{d}{k} x_h .$$

Ponendo $(k, x_1, \ldots, x_{n+i}) = K_1$ si ha $K \cdot \frac{d}{K_1} K = 0$, cioè che K è 0-dimensionale e separabile su K_1. Ne segue che fra gli elementi $x_1, \ldots, x_{n+i}$ debbono trovarsi n elementi algebricamente indipendenti sopra k. Supponiamo per esempio che $K_2 = (k, x_1, \ldots, x_n)$ sia n-dimensionale sopra k. Esiste allora (ved. 26) fra K e K_2 un massimo corpo intermedio separabile $K_3 = (K_2, y)$. Essendo K puramente inseparabile sopra K_3 e valendo, di seguito all'ipotesi (*)

$$K \cdot \frac{d}{K_3} K = \sum_{h=n+1}^{n+i} K \cdot \frac{d}{K_3} x_h$$

il corpo K può generarsi (ved. 35) nel modo seguente

$$(**) \qquad K = (K_3, x_{n+1}, \ldots, x_{n+i}) = (K_2, y, x_{n+1}, \ldots, x_{n+i}).$$

Poiché i corpi (K_2, y) e (K_2, x_{n+1}) sono 0-dimensionali sopra K_2 mentre uno di essi è separabile, si può applicare il teorema **29** scrivendo $(K_2, y, x_{n+1}) = (K_2, z)$ cosicché da (**) risulta

$$K = (K_2, z, x_{n+2}, \ldots, x_{n+i}) = (k, x_1, \ldots, x_n, z, x_{n+2}, \ldots, x_{n+i}).$$

II. Se è possibile generare il corpo K con m elementi $y_1, \ldots, y_m$ sopra k: $K = (k, y_1, \ldots, y_m)$, si ha $K \cdot \frac{d}{k} K = \sum_{i=1}^{m} K \cdot \frac{d}{k} y_i$ e perciò $m \ge \text{rango}\, K \cdot \frac{d}{k} K = n + i$.

C. d. d.