Bollettino
Unione Matematica Italiana

I. Barsotti

Osservazioni elementari intorno al differente di un corpo o di un'algebra sopra un corpo algebrico, o sopra un corpo di funzioni algebriche di una variabile

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **3** (1948), n.3, p. 223–227.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1948_3_3_3_223_0>

Bollettino dell'Unione Matematica Italiana, Zanichelli, 1948.

Osservazioni elementari intorno al differente di un corpo o di un'algebra sopra un corpo algebrico, o sopra un corpo di funzioni algebriche di una variabile.

Nota di I. BARSOTTI (a Roma).

Sunto. - *Si mostrano per via elementare i motivi delle analogie o diversità di comportamento del differente nei vari casi elencati nel titolo, dando anche il legame col numero di diramazione di una superficie di* RIEMANN; *si dà una semplice dimostrazione dell' espressione del discriminante di un' algebra.*

In tutta la presente nota si terranno fisse le seguenti notazioni: C denota un corpo algebrico di grado finito, ossia un prolungamento algebrico di grado finito del corpo razionale;

k denota un corpo di caratteristica zero, e $k(x)$ un suo prolungamento trascendente puro;

F denota un prolungamento algebrico di grado finito di C, e quindi è esso stesso un corpo algebrico di grado finito;

K denota un prolungamento algebrico di grado finito su $k(x)$,

(1) Si noti come l'impossibilità di soddisfare, almeno per questa via, l'equazione (7) per n pari, si accordi con la congettura di EULERO, secondo la quale è irresolubile in interi l'equazione:

$x^4 = y^4 + z^4 + t^4$ (DICKSON, « History », pag. 648. L. EULERO, « Comm. Arith. », I, 473; Op. om., (1), III, pag. 211) e quindi è un corpo di funzioni algebriche di una variabile, e si supporrà che abbia k come corpo delle costanti;

S denota un' algebra semplice normale a base finita su C.

I corpi C, $k(x)$, F, K soddisfano alle tre condizioni di E. NOETHER [9] (¹), che assicurano che in essi vale la fattorizzazione unica degli ideali come prodotto di ideali primi, e valgono le altre solite regole di aritmetica per gli ideali. Si intende che gli ideali vanno considerati rispetto all' anello $\mathfrak{g}$ degli interi di C, oppure a quello $k[x]$ degli « interi » di $k(x)$.

Si indicherà con $\mathfrak{o}$ l' anello degli elementi di F che sono interi rispetto a $\mathfrak{g}$; con $\mathfrak{o}_x$ l' anello degli elementi di K che sono interi rispetto a $k[x]$; con $\mathfrak{S}$ una schiera massima (²) di S rispetto a $\mathfrak{g}$ [3]; con $\mathfrak{D}_F$, $\mathfrak{D}_x$, $\mathfrak{D}$ rispettivamente i differenti di $\mathfrak{o}$, $\mathfrak{o}_x$, $\mathfrak{S}$ rispetto a $\mathfrak{g}$, $k[x]$, $\mathfrak{g}$.

Se $\mathfrak{P}$ è un ideale primo di $\mathfrak{o}$, e $\mathfrak{p} = \mathfrak{P} \frown \mathfrak{g}$, si ha $\mathfrak{p}\mathfrak{o} = \mathfrak{P}^e\mathfrak{Q}$, ove $e \geq 1$, mentre $\mathfrak{Q}$ è un ideale di $\mathfrak{o}$, primo con $\mathfrak{P}$; e è l'*ordine di ramificazione* di $\mathfrak{P}$; relazioni analoghe valgono in K od S; gli ordini di ramificazione dei primi di $\mathfrak{o}$ sono tutti eguali ad 1, eccetto al più che per un numero finito di primi, i primi *ramificati*. Nel caso di K, ogni primo di $\mathfrak{o}_x$ definisce una valutazione, e quindi un divisore di K che si indicherà ancora con $\mathfrak{P}$; si ottengono in questo modo tutti e soli i divisori di K che sono al finito rispetto ad x; il numero $e - 1$ è conosciuto anche come il *numero di ramificazione* del divisore $\mathfrak{P}$ rispetto ad x. Se si sceglie x in modo che nessuno dei divisori all' infinito sia ramificato, allora la somma di tutti gli $e - 1$, al variare di $\mathfrak{P}$, è il *numero di ramificazione* di K rispetto ad x, mentre $\mathfrak{D}_x' = \prod_{\mathfrak{P}} \mathfrak{P}^{e-1}$ è il *divisore di ramificazione* di K rispetto ad x; si supporrà nel seguito di essersi posti appunto in questo caso.

È ben noto (cfr. [3] [5] [2]) il seguente risultato:

$\mathfrak{D}_F$ (*risp.* $\mathfrak{D}_x$, $\mathfrak{D}$) *è il prodotto di tutti i primi ramificati di* $\mathfrak{o}$ (*risp. di* $\mathfrak{o}_x$, *di* $\mathfrak{S}$), *ciascuno elevato ad una potenza con esponente* e *maggiore od eguale al rispettivo numero di ramificazione* $e - 1$.

Nel caso generale non è possibile precisare maggiormente tali esponenti per via elementare. La precisazione è però possibile nel caso di K o di S; per questo secondo caso essa è stata data esat-

(¹) I numeri in parentesi quadre si riferiscono alla bibliografia posta alla fine della nota.

(²) Seguendo l' ALBERT, preferisco chiamare *schiera* ciò che viene comunemente indicato con la parola *ordine*, per evitare confusioni con l' ordine di S su C, che è il numero degli elementi di una base di S su C.

tamente la prima volta in [7], ed è: $c = e - 1$. La stessa precisazione vale nel caso di K, e si può perciò esprimere anche così:

divisore di ramificazione $\mathfrak{D}_x' =$ differente $\mathfrak{D}_x$.

Questo secondo caso è di per sè importantissimo, perchè $\mathfrak{D}_x$, diviso per il quadrato del denominatore $\mathfrak{N}$ di x, dà un rappresentante della classe canonica ([3]).

Mi pare che in genere non si sottolinei abbastanza questa identità: mentre nelle trattazioni classiche [6] si parla esclusivamente di $\mathfrak{D}_x'$, in quelle moderne [8] è $\mathfrak{D}_x$ che si usa per costruire la classe canonica. Reputo quindi non inutile mostrare elementarmente dove nasce precisamente la differenza di comportamento fra F, K ed S; si troverà che tale differenza risiede:

1. – Per K nel fatto che $\mathfrak{o}_x$ contiene tutto il corpo k (mentre nel caso di F, $\mathfrak{o}$ non contiene nessun corpo);

2. – Per S, nel fatto che un' algebra semplice normale sopra un corpo locale contiene un sottocorpo massimo non ramificato.

Si ricordi infatti la definizione del differente, e si ragioni, per fissare le idee, su F; se $\mathfrak{Q}$ è un ideale di $\mathfrak{o}$, si indichi con $T(\mathfrak{Q})$ quell' ideale di g che consta dell' insieme delle $T(a)$ con $a \varepsilon \mathfrak{Q}$, ove T indica la traccia da F a C (risp. da K a $k(x)$; risp. la traccia ridotta da S a C); l' insieme degli $a \varepsilon F$ tali che $T(a\mathfrak{o}) \leq \mathfrak{g}$ è il *complementare* $\tilde{\mathfrak{o}}$ di $\mathfrak{o}$, e si ha $\mathfrak{D}_F = \tilde{\mathfrak{o}}^{-1}$.

Suppongasi che sia $c > e - 1$, ossia $c \geq e$, e ci si ponga nel caso di F (o K): si supponga dapprima F normale su C; da $c \geq e$ segue $\mathfrak{D}_F \leq \mathfrak{P}^e$, e perciò, se $\mathfrak{P}'$ è un qualsiasi coniugato di $\mathfrak{P}$ nel gruppo di Galois di F su C, si ha anche $\mathfrak{D}_F \leq \mathfrak{P}'^e$; ma, a causa della normalità, è $\mathfrak{p}\mathfrak{o} = \mathfrak{P}^e\mathfrak{P}'^e \ldots$, onde $\mathfrak{D}_F \leq \mathfrak{p}\mathfrak{o}$; di qui segue successivamente: $\tilde{\mathfrak{o}} \geq \mathfrak{p}^{-1}\mathfrak{o}$, $\mathfrak{p}^{-1}T(\mathfrak{o}) = T(\mathfrak{p}^{-1}\mathfrak{o}) \leq T(\tilde{\mathfrak{o}}) \leq \mathfrak{g}$,

$$T(\mathfrak{o}) \leq \mathfrak{p}. \tag{1}$$

Basterebbe perciò trovare un intero di F la cui traccia sia fuori di $\mathfrak{p}$, per essere giunti ad un risultato assurdo; ora, ciò non è sempre possibile nel caso di F; si può peraltro dire qualcosa nel caso in cui $\mathfrak{p}$ non divida il grado t di F su C; infatti è $T(1) = t$, che non è elemento di $\mathfrak{p}$. Ci si ponga invece nel caso di K; allora $T(t^{-1}) = 1$, che non è elemento di $\mathfrak{p}$, e $t^{-1} \varepsilon \mathfrak{o}_x$; perciò la (1) è falsa, e $c = e - 1$.

La ipotesi che K sia normale su $k(x)$ si elimina nel solito modo, che è il seguente. Sia: $\overline{K}$ un corpo delle radici di K su $k(x)$; $\mathfrak{d}$ il differente di $\overline{K}$ rispetto a K; $\overline{\mathfrak{D}}$ quello di $\overline{K}$ rispetto a $k(x)$; si sa

([3]) Se k non ha caratteristica zero, la precedente precisazione può non essere valida; cfr. per es. [4], pag. 42.

allora che $\mathbf{D} = \mathbf{d}\mathbf{D}_x$. Se $\bar{\mathbf{o}}$ è l'anello degli interi di $\bar{K}$ rispetto ad $\mathbf{o}_x$ (e quindi rispetto a $k[x]$), sia $\bar{\mathbf{P}}$ un primo di $\bar{\mathbf{o}}$, $\mathbf{P} = \bar{\mathbf{P}} \frown \mathbf{o}_x$,

$$\mathbf{p} = \mathbf{P} \frown k[x] = \bar{\mathbf{P}} \frown k[x],$$

e si abbia:

$\mathbf{p}\mathbf{o}_x = \mathbf{P}^e \times$ ideali primi con $\mathbf{P}$,

$\mathbf{P}\bar{\mathbf{o}} = \bar{\mathbf{P}}^{\bar{e}} \times$ ideali primi con $\bar{\mathbf{P}}$, e quindi

$\mathbf{p}\bar{\mathbf{o}} = \bar{\mathbf{P}}^{e\bar{e}} \times$ ideali primi con $\bar{\mathbf{P}}$. Allora si è visto che $\bar{\mathbf{D}} = \bar{\mathbf{P}}^{e\bar{e}-1} \times$ ideali primi con $\bar{\mathbf{P}}$; poichè $\bar{K}$ è normale, oltre che su $k(x)$, anche su K, si ha analogamente che

$\mathbf{d} = \bar{\mathbf{P}}^{\bar{e}-1} \times$ ideali primi con $\bar{\mathbf{P}}$; quindi:

$\mathbf{D}_x\bar{\mathbf{o}} = \bar{\mathbf{D}}\mathbf{d}^{-1} = \bar{\mathbf{P}}^{e\bar{e}-1-\bar{e}+1} \times$ (ideali primi con $\bar{\mathbf{P}}$)$=\bar{\mathbf{P}}^{\bar{e}(e-1)} \times$ ideali primi con $\bar{\mathbf{P}}$; se si considerano tutti i divisori primi $\bar{\mathbf{P}},\dots,\bar{\mathbf{P}}_n$ di $\mathbf{P}\bar{\mathbf{o}}$, si ottiene perciò:

$\mathbf{D}_x\bar{\mathbf{o}} = (\bar{\mathbf{P}}^{\bar{e}}\dots\bar{\mathbf{P}}_n^{\bar{e}})^{e-1} \times$ (ideali primi con $\bar{\mathbf{P}},\dots,\bar{\mathbf{P}}_n$)$=\mathbf{P}^{e-1}\bar{\mathbf{o}} \times$ ideali primi con $\mathbf{P}\bar{\mathbf{o}}$, che dimostra completamente l'asserto.

Si consideri ora l'algebra S. Il ragionamento si semplifica molto passando da C a C_p (completamento di C mediante la valutazione indotta da $\mathbf{p}$), e da S ad $S_p = S \times C_p$. Si indichi con $\mathfrak{g}_p$ l'anello degli interi di C_p, con $\mathfrak{S}_p$ il completamento di $\mathfrak{S}$, con $\mathbf{D}_p$ il differente di $\mathfrak{S}_p$, e si continuino ad indicare con $\mathbf{p}$, $\mathbf{P}$ gli (unici) ideali primi di $\mathfrak{g}_p$, $\mathfrak{S}_p$.

Secondo una osservazione fatta in [7], la potenza di $\mathbf{P}$ che divide $\mathbf{D}$ è la stessa che divide $\mathbf{D}_p$, e quindi basta calcolare quest'ultima. Essendo S_p normale su C_p, si ha semplicemente [3] $\mathbf{p}\mathfrak{S}_p = \mathbf{P}^e$; ed ancora $\mathbf{D}_p = \mathbf{P}^c$, $c \geq e-1$. Se fosse $c \geq e$, ossia $\mathbf{D}_p \leq \mathbf{P}^e$, si avrebbe: $\mathbf{D}_p \leq \mathbf{p}\mathfrak{S}_p$, $\tilde{\mathfrak{S}}_p \geq \mathbf{p}^{-1}\mathfrak{S}_p$, e proseguendo si tornerebbe alla analoga della (1), e cioè alla

$$T(\mathfrak{S}_p) \leq \mathbf{p};$$

si tratta di ridurre questa ad un assurdo; ora [1] S_p contiene un sottocorpo massimo non ramificato W; essendo W non ramificato, il suo differente su C_p è l'ideale unità, e quindi W contiene un intero z la cui traccia da W a C_p (che si indicherà con T_W) è eguale ad 1. $T_W(z)$ è il secondo coefficiente di un polinomio monico $\varphi(x)$, di grado t eguale al grado di W e quindi di S_p (od anche di S), che è una potenza del polinomio minimo $\psi(x)$ di z; ma anche la funzione principale $f(x)$ di z come elemento di S_p, il cui secondo coefficiente è $T(z)$, ha grado t ed è [1] potenza di $\psi(x)$; quindi $f(x) = \varphi(x)$, e $T(z) = T_W(z) = 1$; poichè con opportuni autoisomorfismi interni si può fare in modo che z sia in $\mathfrak{S}_p$, si deduce ancora $c = e-1$, come richiesto.

In questo secondo caso si può calcolare $\mathbf{D}$ in base agli invarianti locali di S. Si sa infatti che se S_p ha grado t ed indice n_p. ossia se $S_p = M_p \times D_p$, con M_p regolare e D_p divisoria di grado n_p, allora $\mathfrak{p}$ ha, rispetto a D_p, ordine di ramificazione n_p, che resta invariato in S_p, dato che [3] un ideale primo di una schiera massima di D_p resta primo quando venga esteso ad una schiera massima di $M_p \times D_p$; perciò

$$\mathfrak{D}_p = \mathfrak{P}^{n_p-1}, \quad \text{ed allora } \mathfrak{D} = \Pi\, \mathfrak{P}^{n_p-1}.$$

Si può completare per questa via il risultato di [7], calcolando il discriminante $\mathfrak{d}$ di S su C; esso è definito come la norma N_1 del differente. Se si tiene presente che [3]

$$N_1(\mathfrak{P}) = \mathfrak{p}^{t^2/n_p},$$

si ha:

$$\mathfrak{d} = N_1(\Pi\, \mathfrak{P}^{n_p-1}) = \Pi\, (N_1(\mathfrak{P}))^{n_p-1} = \Pi\, \mathfrak{p}^{(n_p-1)t^2/n_p} = (\Pi\, \mathfrak{p}^{t(1-1/n_p)})^t.$$

Si ritrova così il noto risultato [3] secondo cui $\mathfrak{d}$ è potenza t–esima di un ideale (l'*idèale fondamentale* di S), e per quest'ultimo si trova l'espressione $\mathfrak{d}' = \Pi\, \mathfrak{p}^{t(1-1/n_p)}$. Se S fosse semplice normale sopra un corpo di funzioni algebriche di una variabile, il ragionamento ed il risultato sarebbero esattamente gli stessi se fosse soddisfatta una delle seguenti ipotesi:

1. – Il corpo delle costanti è finito (cfr. [10]).
2. – Il corpo delle costanti è algebricamente chiuso.

Nel caso 2 il risultato sarebbe banale, perchè i $\mathfrak{D}_p$ sarebbero tutti eguali ai $\mathfrak{S}_p$, e quindi $\mathfrak{D} = \mathfrak{S}$.

BIBLIOGRAFIA

[1] ALBERT, *Structure of algebras.* (« Amer. Math. Soc. Coll. Publ. », 1939)

[2] BIANCHI, *Teoria dei numeri algebrici,* (1923).

[3] DEURING, *Algebren.* (« Ergeb. der Mathem. », 4, 1935).

[4] HASSE, *Theorie der relativ-zyklischen algebraischen funktionenkörper, insbesondere bei endlichen konstantenkörper.* (« Journ. für die reine und angew. Mathem. », 172, 1935, p. 37).

[5] HECKE, *Vorlesungen über die theorie der algebraischen zahlen,* (1923).

[6] HENSEL e LANDSBERG, *Theorie der algebraischen funktionen einer variabeln,* (1902).

[7] REICHARDT, *Die diskriminante einer normalen einfachen algebra.* (« Journ. für die reine und angew. Mathem. », 173, 1935, p. 31).

[8] F. K. SCHMIDT, *Zur arithmetischen theorie der algebraischen funktionen I.* (« Math. Zeit. », 41, 1936, p. 415).

[9] van der WAERDEN, *Moderne algebra.* (1930, opp. 1940).

[10] WITT, *Riemann-Rochscher satz und Z-funktion im hyperkomplexen.* (« Math. Ann. », 110, 1935, p. 12).