Rendiconti
del
Seminario Matematico
della
Università di Padova

Salvatore Cherubino

Sulla teoria delle equazioni algebriche

Rendiconti del Seminario Matematico della Università di Padova, tome 6 (1935), p. 1-8

<http://www.numdam.org/item?id=RSMUP_1935__6__1_0>

SULLA TEORIA DELLE EQUAZIONI ALGEBRICHE

di SALVATORE CHERUBINO *a Messina*

Un recente lavoro di Colucci [1] m' invita a tornare sopra un mio teorema [2] che qui completo con qualche osservazione che valga a metterne in rilievo l' interesse ed indicando due casi di eccezione [3], che ne precisano la portata.

Aggiungo alcune proprietà delle trasformate razionali delle equazioni binomie, che, pur essendo indipendenti dalle osservazioni di cui sopra, hanno con queste in comune lo scopo principale e non mancano d' espressività.

1. Avvertiamo una volta per tutte:

che le equazioni, i polinomi, le funzioni razionali, le forme quadratiche e le matrici qui considerate sono sempre (a coefficienti) reali;

che con $\overline{\alpha}$ indichiamo il numero complesso coniugato di α;

che dicendo che i numeri α e β sono distinti e non complessi coniugati intendiamo che le coppie non ordinate $(\alpha, \overline{\alpha})$,

(1) *Sopra i polinomi definiti* [Atti Accad. Napoli, vol. XX, serie 2ª, n. 12 (1934 - XII)).

(2) *Su le forme associate ai polinomi* [Questi Rend., anno II, n. 2 (1931 - IX)] n. 2.

(3) Il primo di essi era già stato da me rilevato sin dal 1931 ed indicato, a mano, sugli estratti della Nota precedente. Con l' occasione avverto che nella stessa Nota, nell' enunciato del teorema del n. 6 a pag. 12, invece di dirsi.... « *sono associate tutte le forme* » etc., deve dirsi « *è associata una stessa forma* », etc.

$(\beta, \bar{\beta})$ non coincidono, quindi che, se almeno uno dei 2 numeri è reale, sia semplicemente $\alpha \neq \beta$;

che quando diciamo che un polinomio è reduttibile o non vogliamo intendere che lo è l'equazione che si ha eguagliandolo a zero e che la reduttibilità o l'irreduttibilità han luogo nel campo di razionalità definito dai coefficienti (o in altro esplicitamente dichiarato).

Osserviamo infine che, com'è ovvio, due polinomi sono linearmente dipendenti allora e solo che differiscono per un fattore costante cioè quando e soltanto quando posseggono le stesse radici con le stesse molteplicità.

2. Un polinomio $f(x)$, di grado $2m$, soddisfi all'identità

$$f(x) = \chi_1(x)^2 - \chi_2(x)^2 \tag{1}$$

con χ_1 e χ_2 polinomi di grado non superiore ad m, linearmente indipendenti. Ponendo

$$\varphi(x) = \chi_1(x) + \chi_2(x), \quad \psi(x) = \chi_1(x) - \chi_2(x) \tag{2}$$

segue l'altra identità

$$f(x) = \varphi(x) \cdot \psi(x) \tag{3}$$

coi polinomi φ e ψ entrambi di grado m e linearmente indipendenti.

Viceversa, da quest'ultima, posto le (2) si risale all'identità (1). Ed avendo supposto φ e ψ di grado m e linearmente indipendenti, saranno tali anche χ_1 e χ_2 (uno solo necessariamente di grado m, l'altro di grado $\leq m$).

Osservisi che l'identità (3), con le condizioni imposte a φ e ψ, si verifica allora e solo che le $2m$ radici di $f(x)$ siano ripartibili in 2 gruppi *non coincidenti*, ciascuno di m radici, e tali che se la radice α appartiene a un gruppo vi appartiene anche la radice $\bar{\alpha}$. Per la non coincidenza dei 2 gruppi – che diciamo gruppo φ e gruppo ψ – occorre ovviamente che vi sia (almeno) una radice α che (insieme ad $\bar{\alpha}$, se α non è reale) appartenga ad uno solo dei due gruppi, oppure figuri, per es., nel primo più volte che nel secondo. Allora esisterà anche una radice β che (insieme a $\bar{\beta}$ se β non è reale) appartiene soltanto all'altro gruppo oppure figura nel secondo più volte che nel primo.

Ciò esige che $f(x)$ possegga (almeno) due radici distinte e non complesse coniugate (le radici α e β di poco fa).

Aggiungasi, che quando m è dispari, ciascun gruppo φ o ψ deve necessariamente possedere (almeno) una radice reale, sicchè, pur verificandosi la condizione precedente, la ripartizione richiesta è impossibile nei 2 casi seguenti:

1.° quando m è dispari ed $f(x)$ è privo di radici reali,

2.° quando m è ancora dispari ed $f(x)$ possiede due (sole) radici reali coincidenti con le rimanenti $2(m-1)$ imaginarie ed esauribili con la stessa coppia di numeri coniugati (nel qual caso i 2 gruppi φ e ψ coincidono).

In ogni altra eventualità [4] la ripartizione è sempre effettuabile, onde può affermarsi che:

[4] Le altre sono le seguenti:

a) m è dispari e vi sono 2 radici reali distinte con le rimanenti $2m-2$ imaginarie, oppure 2 radici reali coincidenti e $2m-2$ imaginarie, ma con 2 coppie distinte di radici coniugate.

b) m è ancora dispari e vi sono $2h \geq 4$ radici reali, quindi $p = m-h \geq m-2$ coppie di radici immaginarie coniugate. Allora potrà scegliersi $p'+p''=p$ e $2p' < m$ e porre p' coppie di radici imaginarie in φ, p'' in ψ, (se $2h \leq m+1$ basta prendere $p' = \frac{m-1}{2}$, $p'' = \frac{m+1}{2} - h$; se $2h > m+1$, basta prendere $p' = m-h$, $p''=0$].

c) m è pari e non vi sono radici reali (ma almeno due coppie coniugate non coincidono).

d) m è ancora pari e vi sono $2h \geq 2$ radici reali, quindi $p = m-h < m$ coppie di radici imaginarie coniugate. Si potrà allora porre $p'+p''=p$ con $p' > p''$ e $2p' \geq m$, $2p'' < m$ etc., come nel caso *b*) [Se $2h < m$, si prenda $p' = \frac{m}{2}$, $p'' = \frac{m}{2} - h$; se $2h \geq m$, si prenda $p' = m-h$, $p''=0$].

e) m è qualunque e le radici sono tutte reali (ma due almeno sono distinte).

La dimostrazione sopra esposta coincide, salvo la forma e la maggiore estensione, con quella della Nota cit. [2].

Salvo i due casi limiti sopra indicati, ogni polinomio di grado $2m$ che possegga (almeno) due radici distinte non complesse coniugate è sempre differenza dei quadrati di 2 polinomi di grado non superiore ad m e linearmente indipendenti.

OSSERVAZIONE. Se la indipendenza lineare di χ_1 e χ_2, quindi quella di φ e ψ, non è più richiesta, non occorre fare alcuna ipotesi su $f(x)$. E per ottenere che il grado di χ_1 e χ_2 sia sempre non superiore ad m, basta escludere soltanto il primo dei 2 casi limiti (quello di m dispari e delle radici tutte immaginarie) ([5]). La dimostrazione di questo fatto è ovviamente analoga alla precedente, ma riesce molto più semplice e più breve.

3. Il risultato precedente, nella mia Nota cit. ([2]), era stato anche presentato sotto una forma più espressiva, che ne precisa l'interesse. Val la pena di riportarla, per avere l'opportunità di aggiungere una non inutile osservazione.

Indicando con y lo $(m+1)$- complesso orizzontale $(y_0, y_1, \ldots, y_m)$ e con a una matrice simmetrica di ordine $m+1$, si dice che la forma quadratica

$$\varphi(y_0, y_1, \ldots, y_m) = y \cdot a \cdot y_{-1} \text{ } ([6]) \tag{4}$$

è *associata* ad $f(x)$ quando ha luogo l'identità

([5]) Questa osservazione esprime un fatto più generale di quello segnalato da A. COLUCCI fra le pagg. 7 ed 8 della Nota cit. ([1]) (raggiunto dall A. servendosi di una trasformata di TSCHIRNHAUSEN e di un'osservazione sui determinati simmetrici a matrice). A questo proposito aggiungo che, a causa di un equivoco sul significato della frase « radici distinte non complesse coniugate » COLUCCI (com'egli scrive pregandomi di avvertirlo) aveva erroneamente creduto che il suo risultato emendasse l'enunciato sopra esposto, contenuto nella mia Nota cit. ([2]). Nuovo, invece, potrebbe dirsi il risultato successivo della nota di COLUCCI, (alla stessa pag. 8): questo è però anch'esso contenuto nella dimostrazione di cui sopra, pel caso che i 2 polinomi χ_1 e χ_2 possano superare il grado m.

([6]) Con y_{-1} si indica l'$(m+1)$- complesso verticale che ha gli stessi elementi di y. In generale, con a_{-1} si indica la matrice trasposte di a. Qui facciamo uso, più sistematicamente, del simbolismo del calcolo con matrici.

$$(5) \qquad f(x) = X \cdot a \cdot X_{-1} \;, \quad X = (x^m, \, x^{m-1}, \ldots, \, x, \, 1)$$

cioè l'altra

$$(5') \qquad f(x) = \varphi\,(x^m, \, x^{m-1}, \ldots, \, x, \, 1),$$

che si riducono entrambe a relazioni lineari fra i coefficienti di φ e di $f(x)$. Se φ è di caratteristica due ed indice d'inerzia zero, cioè se φ è differenza dei quadrati di due forme lineari in $y_0, \ldots, y_m$, linearmente indipendenti, $f(x)$ risulta differenza dei quadrati di due polinomi di grado non superiore ad m e linearmente indipendenti.

La proprietà, causa la identità (5), è ovviamente invertibile, quindi:

Sotto le stesse ipotesi (e le stesse eccezioni limiti) *dell' enunciato precedente*, $f(x($ *ammette una forma quadratica associata di caratteristica due ed indice d' inerzia zero. E viceversa* (7).

Orbene, la più generale matrice (simmetrica) dei coefficienti di una forma quadratica di caratteristica due ed indice d' inerzia zero, *a meno dell' ordine delle righe* (e delle colonne), si scrive (8):

$$(6) \qquad \left(\begin{array}{c|c} D & D \cdot \lambda \\ \hline \lambda_{-1}\, D & \lambda_{-1}\, D \cdot \lambda \end{array} \right)$$

essendo D la più generale matrice simmetrica, di ordine 2, a determinante negativo e λ la più generale matrice a 2 righe ed $m - 1$ colonne. Perciò, se nella (5) si prende per a la matrice (6), $f(x)$ risulta il più generale polinomio di grado $2m$ soddisfacente alla proposizione del n. 2, al di fuori dei soliti 2 casi eccezionali.

(7) Segue che, ogni qual volta si trovi una forma quadratica, associata ad $f(x)$, che abbia caratteristica 2 ed indice d' inerzia zero, la riduzione di questa a forma canonica abbassa la risoluzione dell' equazione $f(x) = 0$ a quella di due equazioni di grado $m\,[\varphi(x) = 0$ e $\psi(x) = 0]$.

(8) Cfr. la mia Nota: *Un'applicazione del calcolo di matrici alla teoria delle forme quadratiche* [Rend. Ist. Lomb., vol. LXII, 1929], n. 1.

Ma anche questi possono essere rappresentati sotto la forma generale (5), lasciando la matrice D completamente arbitraria (ma simmetrica, di 2° ordine e non nulla). Ed invero, se $f(x)$ è privo di radici reali, esso (a meno di un fattor costante) è necessariamente somma dei quadrati (9) di due polinomi di grado $\leq m$, linearmente indipendenti, sicchè per includere la prima eccezione, occorre e basta poter prendere anche $|D|>0$. E se $f(x)$ presenta la seconda eccezione, esso è necessariamente quadrato di un polinomio di grado m, sicchè per includere questa eccezione basterà poter prendere $|D|=0$, nel qual caso la caratteristica della (6) è uno (sarebbe zero solo se D fosse nulla).

Concludendo:

se a *è la più generale matrice simmetrica di ordine* $m+1$ *e caratteristica* ≤ 2 (cioè assegnata dalla (6) con D matrice non nulla ma simmetrica e di ordine 2) *nelle* (5) *è rappresentato il più generale polinomio di grado* $2m$ (10).

4. Passiamo alle trasformate razionali dell'equazione

$$y^{n+1}-A=0. \tag{7}$$

Esse, com'è noto, si ottengono *tutte* eliminando y fra questa e la relazione

$$x=a_0 y^n+a_1 y^{n-1}+\ldots+a_n \tag{8}$$

al variare di $a_0, a_1\ldots, a_n$ in tutti i modi possibili (nel corpo reale).

(9) Cfr. l'altra Nota: *Sulle decomposizioni in somme di quadrati dei polinomi definiti o semidefiniti.* [Ibidem], n. 1 e).

(10) Si noti che nella (6) vi sono $2m+1$ quantità (reali) arbitrarie, $2(m-1)$ in λ e 3 in D, cioè tante quanti sono i coefficienti di $f(x)$. Si tenga anche presente che, come del resto abbiamo già osservato altrove, se si impone la sola condizione $|D|>0$ la (5) ci dà il più generale polinomio definito o semidefinito e che imponendo solo l'altra $|D|=0$ scriviamo il più generale polinomio quadrato di un altro.

Applicando il metodo di Sylvester, dopo facile riduzione, si ottiene come trasformata

$$(9) \qquad F(a_0, a_1, \dots, a_n, A; x) = f(x) =$$

$$= \begin{vmatrix} a_0 & a_1 \dots & a_{n-1} & a_n - x \\ a_1 & a_2 \dots & a_n - x & A a_0 \\ \vdots & & \vdots & \vdots \\ a_n - x & A a_0 \dots & A a_{n-2} & A a_{n-1} \end{vmatrix} = 0$$

che si ottiene dal *circolante* dei ceefficienti $a_0, a_1, \dots, a_n$ togliendo x dagli elementi della diagonale secondaria e moltiplicando per A tutti i termini al disotto di detta diagonale.

Se $n+1$ è dispari, la (7) ammette una sola radice reale, quindi $f(x)$ ne ammetterà anch'essa una sola oppure, oltre questa, una o più coppie di radici reali coincidenti. Se $n+1$ è pari, la (7) possiede due o nessuna radice reale, secondo che $A \gtrless 0$; in corrispondenza, $f(x)$ possiederà una o nessuna coppia di radici reali distinte oppur no, mentre le altre radici risulteranno, a coppie, imaginarie coniugate o reali coincidenti. Per ogni altro riguardo, con opportuna scelta dei coefficienti $a_0, a_1, \dots, a_m$, le radici di $f(x)$ possono fissarsi ad arbitrio. Quindi, per $n+1$ pari, secondo che $A \gtrless 0$, la (9) ci dà la più generale equazione le cui coppie di radici sono immaginarie coniugate o reali coincidenti, salvo una coppia che dev'essere di radici reali non necessariamente coincidenti, oppure ci fornisce il più generale polinomio definito o semidefinito, di quel grado ([11]).

Ricordiamo, a questo punto, che un notevole risultato del Capelli ([12]) ci assicura che la (7) è irreduttibile, nel campo di

([11]) Questo risultato, per $A = \pm 1$, è stato ottenuto, allo stesso modo come qui sopra, da A. Colucci, nella Nota cit. ([1]), *n.* 6. Si tenga presente che quando quest' A. dice definito intende definito o semidefinito.

([12]) *Sulla reduttibilità delle equazioni algebriche.* [Rend. Acc., Napoli, 1897-1898, note I, II e III]. Cfr. anche *Giornale di Matematiche,* Napoli, vol. XLI, (1904).

razionalità R definito dai numeri $a_0, a_1, \dots, a_n$, A, allora e solo che A non è potenza di un numero di R, con esponente divisore di $n+1$, e se inoltre, quando $n+1$ sia multiplo di 4, non possa porsi $A = -4\,\alpha^4$, con α appartenente ad R.

Se la (7) è reduttibile in R, è certo tale anche $f(x)$. Se la (7) è irreduttibile, la (9) lo sarà anch'essa, oppure, com'è noto, avrà le sue radici tutte della stessa molteplicità $r > 1$. Perciò, per assicurarsi della irreduttibilità di $f(x)$, oltre a soddisfare alle condizioni del Capelli, occorre e basta assicurarsi che non si annulli il suo discriminante.

Si può dunque enunciare:

Affinchè il polinomio $f(x)$ *assegnato dalla* (9), *supposto già privo di radici multiple* ([13]), *risulti definito* (cioè privo di radici reali) *ed irreduttibile nel campo di razionalità* R *assegnato da* $a_0, a_1, \dots, a_n$, *occorre e basta scegliere* ($n+1$ *pari ed*) A *in questo campo evitando i valori positivi, le potenze dei numeri di* R *con esponenti divisori di* $n+1$ *e, quando* $n+1$ *sia multiplo di* 4, *i valori del tipo* $-4\,\alpha^4$, *con* α *appartenente ad* R.

Una condizione necessaria e sufficiente perchè la (9) dia un polinomio definito, non necessariamente irreduttibile, non sembra esprimibile con altrettanta semplicità ([14]).

([13]) Per $a_0, a_1, \dots, a_m$ *generici*, il discriminante di $f(x)$ dipenderà da A, quindi questa condizione si potrà verificare anch'essa escludendo altri valori per A.

([14]) Per $A < 0$, e se non vi sono radici multiple, $f(x)$ è certo definito, ma non è vero il viceversa. Tutti e soli i polinomi definiti possono però aversi dalla (5) [Cfr. la Nota cit. ([9]), n. 6 *a)*] prendendo per a la più generale matrice caratteristica di una forma quadratica *definita* (non semidefinita).