Bollettino
Unione Matematica Italiana

Bruce E. Meserve

Irriducibilità del risultante e del discriminante.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **8** (1953), n.3, p. 243–252.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1953_3_8_3_243_0>

Bollettino dell'Unione Matematica Italiana, Zanichelli, 1953.

Irriducibilità del risultante e del discriminante.

Nota di BRUCE E. MESERVE (a Urbana, Illinois U.S.A.)

Sunto. - *Si dimostra che il risultante di due polinomi è irriducibile nel più generale campo contenente i coefficienti dei polinomi stessi e, con una opportuna modificazione della definizione di riducibilità, il risultato viene esteso ad ogni anello commutativo con elemento unità.*

Consideriamo due polinomi f, g nella indeterminata x con coefficienti indeterminati. Il risultante $R(f, g)$ e il discriminante $D(f)$ sono polinomi con coefficienti interi. Inoltre è noto che R e D sono ambedue irriducibili nel campo razionale [2; 108–114].

Recentemente ANDREOTTI [1] ha dimostrato che R è irriducibile in ogni campo di caratteristica infinita (1). Essenzialmente il medesimo risultato era stato ottenuto precedentemente da MACAULAY [3; 5] usando un metodo molto simile. La dimostrazione impiega solamente le proprietà formali della moltiplicazione in un anello commutativo. Il presente lavoro contiene una estensione di questo risultato al più generale campo contenente i coefficienti, e, in seguito ad una conveniente modificazione della definizione di riducibilità, ad ogni anello commutativo con elemento unità.

Il metodo formale è vantaggioso non solo perchè è diretto, ma anche perchè esso può essere usato per sistemare la questione della riducibilità in modo completo, cioè in ogni anello commutativo con unità, come è fatto nel presente lavoro. Precisamente, *per ogni intero* k *non negativo, il risultante è irriducibile se i suoi coefficienti sono ridotti modulo* k, $k \neq 1$; *il discriminante è irriducibile se i suoi coefficienti sono ridotti modulo* k, *dove* (2) $k \nmid 4$; *e il discriminante è il quadrato di un polinomio irriducibile se i suoi coefficienti sono ridotti modulo* 2 *o* 4.

1. *Riducibilità.* Sia I_k l'insieme degli interi modulo k, $I_k[X]$ l'anello dei polinomi nelle indeterminate $x_0, x_1, \ldots, x_n$ coi coefficienti in I_k. La definizione, che P è riducibile in $I_k[X]$ se $P = GH$ dove G, H sono $I_k[X]$ e nè G nè H è una unità, non

(1) [*Nota della Redazione*]. Secondo altri autori, forse in maggior numero, si dovrebbe dire « caratteristica zero ». Qui l'A. segue la nomenclatura, ad es., di A. A. ALBERT, *Modern higher Algebra*, Chicago, 1936, p. 30, di BIRKHOFF and MAC LANE, *A survey of modern Algebra*, p. 368.

(2) [*Nota della Redazione*]. La scritturà $a \mid b$ significa: a divide b; la scrittura $a \nmid b$ significa: a non divide b.

soddisfa alle nostre necessità se k è composto. Per esempio, $2x$ sarebbe allora riducibile in I_6. Similmente la definizione che P è riducibile in $I_k[X]$ se (anche dopo aver rimossso divisori dello zero, cioè « fattori irrilevanti ») l'ideale di P è riducibile in $I_k[X]$, è pure non soddisfacente dato che è $x = (2x + 3)(3x + 2)$ in I_6. Pertanto in I_6 la indeterminata x è composta, ed è necessario distinguere tra « composto » e « riducibile ».

« Riducibile » sembra un aggettivo non appropriato se qualche cosa non è ridotto nei due fattori. Classicamente la cosa ridotta è il grado come è detto nelle definizioni in molti ben noti testi. Nel presente lavoro la definizione di riducibile è intesa come segue, in ordine alle proprietà dei polinomi riducibili:

F è riducibile in un anello di polinomi $R[X]$, dove R è un anello commutativo e X è un sistema di indeterminate, se è

$$F = GH, \tag{1}$$

dove G, H sono in $R[X]$, ed è

$$0 < \text{grado } G, \quad 0 < \text{grado } H, \tag{2}$$

e dove per ogni sottosistema x di X (in particolare per l'intero sistema X) è

$$\text{grado}_x F = \text{grado}_x G + \text{grado}_x H.$$

La riducibilità inoltre rimanga attraverso la trasformazione $x_i = x'_i$ per j positivo [3].

Usando queste proprietà ogni polinomio F omogeneo riducibile può essere scritto nella forma $F = GH$ dove grado F = grado G + + grado H. Sia $G = G_1 + G_2$, $H = H_1 + H_2$ dove G_1, H_1 sono polinomi omogenei, ed è

$$\text{grado } G_2 < \text{grado } G_1 = \text{grado } G, \qquad \text{grado } H_2 < \text{grado } H_1 = \text{grado } H.$$

Allora è

$$F = G_1H_1 + G_1H_2 + G_2H_1 + G_2H_2.$$

[3] [*Nota della Redazione*]. Questa condizione, per valori di j diversi da una indeterminata all'altra (e così è adoperata poco dopo), non è conseguenza della condizione precedente.

Si ha infatti, ad es, in $I_6[x, y]$,

$$3xy^2 + 2x^2 + xy + 2x + y = (2x + y)(3xy + x + 1),$$

ed è soddisfatta la condizione della somma dei gradi (totale e parziali); ma se si sostituisce x^2 al posto di x tale condizione, per il grado totale, non è soddisfatta.

Poichè F è omogeneo di grado

$$\text{grado } G + \text{grado } H = \text{grado } G_1 + \text{grado } H_1,$$

abbiamo $G_1H_2 + G_2H_1 + G_2H_2 = 0$ e $F = G_1H_1$.

Quindi ogni polinomio omogeneo riducibile F può essere scritto come prodotto di polinomi omogenei tali che il grado del prodotto sia la somma dei gradi.

Sia F isobarico e riducibile, e sia $F = GH$. Se G ha peso zero, scriviamo $H = H_1 + H_2 + H_3$, dove H_1 è isobarico, *peso* $H_1 =$ *peso* F, *peso* $H_2 <$ *peso* $F <$ *peso* H_3. Allora è $F = GH_1 + GH_2 + GH_3 = GH_1$ dal confronto dei pesi. Se G, H hanno ambedue pesi positivi, facciamo un cambio di indeterminante della forma

$$x_0 = y_0, \quad x_1 = y_1, \quad x_2 = y_2^2, \ \ldots \ x_n = y_n^n.$$

La riducibilità rimane per la proprietà (3) di sopra, e il grado di F nelle y è uguale al peso di F nelle x, Allora il ragionamento usato sopra mostra che è $F = G_1H_1$ dove G_1, H_1 sono omogenei nelle y con $grado_y F = grado_y G_1 + grado_y H_1$, e quindi isobarici nelle x con *peso* $F =$ *peso* $G_1 +$ *peso* H_1.

I due risultati di sopra presi insieme mostrano che, poste per la riducibilità le proprietà di sopra, ogni polinomio riducibile omogeneo, isobarico può essere espresso come prodotto di due polinomi omogenei, isobarici di grado positivo in modo che i gradi e i pesi sono additivi rispetto ai fattori. Questo risultato fornisce la base per le dimostrazioni nel presente lavoro dove è supposto che la riducibilità ha le proprietà dette sopra, in qualsiasi anello $I_\lambda[X]$.

2. *Il risultante.* Il risultante $R(f, g)$ di due polinomi

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_n \qquad (0 < n)$$
$$g = b_0x^m + b_1x^{m-1} + \ldots + b_m \qquad (0 < m)$$

con coefficienti indeterminati può essere espresso come un determinante di ordine $n + m$. Per il nostro proposito è importante la forma esatta del risultante. La specifichiamo come segue. La prima riga del determinante è formata dai coefficienti di f seguiti da $m - 1$ zeri; ciascuna delle $m - 1$ righe successive è ottenuta dalla sua precedente facendo scorrere i coefficienti di f di una colonna a destra, e prendendo i rimanenti elementi eguali a zero. La $(m + 1)^{esima}$ riga è formata dai coefficienti di g seguiti da $n - 1$ zeri; ciascuna delle $n - 1$ righe sucessive è ottenuta dalla sua precedente facendo scorrere i coefficienti di una colonna a destra, e prendendo i rimanenti elementi eguali a zero.

$R(f, g)$ è omogeneo di grado m nei coefficienti di f, omogeneo di grado n nei coefficienti di g, e isobarico. Se è $R = PQ$, anche P e Q sono allora omogenei e isobarici. Allora [4] la presenza dei monomi distinti $a_0^m b_m^n$, $a_n^m b_0^n$ e $a_1^m b_0 b_m^{n-1}$ in R implica che P contiene $a_0^r b_m^s$, $a_n^r b_0^s$, e o $a_1^r b_0 b_m^{s-1}$, onde (poichè P è isobarico) Q è costante, oppure $a_1^r b_m^s$ onde P è costante. Ciò completa la prova che $R(f, g)$ è irriducibile su un campo di caratteristica infinita. Ma di più, poichè ciascuno dei monomi di sopra ha il coefficiente di valore numerico 1 nel polinomio $R(f, g)$, $R(f, g)$ è un polinomio irriducibile nei coefficienti di f e di g quando i suoi coefficienti sono ridotti mod k, dove $1 < k$.

3. *Il discriminante.* La forma del discriminante D di f è data per mezzo del determinante descritto sopra per il risultante, e della relazione $a_0 D = R(f, f')$, dove f' è la derivata di f. Poichè la prima colonna del determinante $R(f, f')$ è divisibile per a_0, il discriminante D_n di un polinomio f di grado n è un polinomio omogeneo di grado $2n - 2$ e di peso $n(n-1)$ nei coefficienti di f. In particolare è $D_1 = 1$ e $D_2 = a_1^2 - 4a_0a_2$. Dato qualsiasi intero k non negativo, $D_1 \pmod k$ è irriducibile se $k \neq 1$; $D_2 \pmod k$ è irriducibile se $k + 4$; e D_2 è il quadrato a_1^2 di un polinomio irriducibile se $k = 2$ o 4.

Il resto di questo lavoro è volto alla dimostrazione di risultati simili per D_n dove è $3 \leq n$. La dimostrazione dipenderà dalla presenza di certi monomi. In particolare noi useremo speciali casi dei due monomi generali seguenti:

$B_j = a_1^j a_j^{n-1} a_n^{n-j-1}$ con coefficiente $\pm (j-1)^{j-1}(n-j)^{n-j}$ quando $1 < j < n$, $\pm (n-j)^{n-j}$ quando $j = 0$ oppure 1; $C_j = a_0^{j-1} a_j^n a_n^{n-j-1}$ con coefficiente $\pm j^j (n-j)^{n-j}$ quando $1 < j < n$.

Questi coefficienti possono essere ottenuti come segue:

Per $1 < j < n$ i fattori a_1^j, a_j^{n-1}, a_n^{n-j-1} di B_j sono distinti. Osserviamo che a_j non compare nelle prime j nè nelle ultime $n - j - 1$ colonne della espressione di D in forma di determinante. Inoltre, nella j^{esima} colonna a_j compare solamente nella prima e nella n^{esima} riga, dalle quali deve essere scelto o un intero o il fattore a_1 di B_j, nella prima e nella seconda colonna rispettivamente. Pertanto per ottenere i singoli monomi B_j dalla espressione del discriminante sotto forma di determinante, deve essere scelto un intero nella prima colonna, l'elemento a_1 nelle successive j colonne, l'elemento a_n nelle ultime $n - j - 1$ colonne, e l'elemento

[4] V. ANDREOTTI, lavoro citato 1.

a_j nelle colonne rimanenti. Abbiamo ormai specificato il fattore di ogni monomio B_j tratto da ciascuna colonna del determinante. Poichè ciascun fattore compare al più due volte in ciascuna colonna, la somma algebrica di tutti i monomi della forma B_j (per ogni j fisso, $1 < j < n$) può essere ottenuta dal seguente prodotto di minori di D

$$\begin{vmatrix} 1 & a_1 \\ n & (n-1)a_1 \end{vmatrix} \cdot \begin{vmatrix} a_1 & a_j \\ (n-1)a_1 & (n-j)a_j \end{vmatrix}^{j-1} \begin{vmatrix} a_j & a_n \\ (n-j)a_j & 0 \end{vmatrix}^{n-j-1} (n-j)a_j$$

ed ha il coefficiente detto sopra.

Si può verificare che non vi sono altri monomi della forma B_j sviluppando il determinante D secondo il procedimento della scelta di un elemento da ciascuna riga e da ciascuna colonna. Per esempio, usando la notazione $a_{r,s}$ per l'elemento della r^{esima} riga e della s^{esima} colonna, troviamo che o a_{11} o a_{n1} deve essere scelto nella prima colonna; a_{12} o a_{n2} nella seconda. Perciò dobbiamo scegliere o $a_{11}a_{n2}$ o $a_{n1}a_{12}$ come è indicato nel primo fattore del prodotto di minori di sopra. Nella terza colonna deve essere scelto o a_{23} o $a_{n+1,3}$, mentre gli elementi scelti da ambedue le righe seconda e $(n+1)^{esima}$ debbono essere multipli di a_1 o di a_j, dato che a_n deve essere scelto dalle ultime $n-j-1$ colonne e quindi dalle righe dalla $(j+1)^{esima}$ alla $(n-1)^{esima}$. Così troviamo che la forma del secondo fattore del prodotto di minori di sopra è unica. Procedendo, abbiamo un metodo per riconoscere che tutti i possibili monomi della forma B_j sono stati inclusi sopra.

Similmente troviamo che B_0 compare in D in un solo modo ed ha il coefficiente $\pm n^n$; B_1 può essere ottenuto sopprimendo il secondo determinante nel prodotto di sopra.

Il coefficiente detto sopra per C_j $(1 < j < n)$ può essere ottenuto dal prodotto

$$\begin{vmatrix} 1 & a_j \\ n & (n-j)a_j \end{vmatrix} \cdot \begin{vmatrix} a_0 & a_j \\ na_0 & (n-j)a_j \end{vmatrix}^{j-1} \begin{vmatrix} a_j & a_n \\ (n-j)a_j & 0 \end{vmatrix}^{n-j-1} (n-j)a_j .$$

La seguente dimostrazione della irriducibilità di D (mod k), dove $k+4$, fa uso dei monomi C_{n-1}, B_0. B_{n-1}, B_1, C_2, B_2, C_{n-2}, C_3 e B_{n-2}, i quali per comodità vengono designati rispettivamente con

$$M_1 = \pm (n-1)^{n-1} a_0{}^{n-2} a^n{}_{n-1}, \qquad M_2 = \pm n^n a_0{}^{n-1} a_n{}^{n-1},$$
$$M_3 = \pm (n-2)^{n-2} a_1{}^{n-1} a_{n-1}^{n-1}, \qquad M_4 = \pm (n-1)^{n-1} a_1{}^n a_n{}^{n-2},$$
$$M_5 = \pm 2^2 (n-2)^{n-2} a_0 a_2{}^n a_n{}^{n-3}, \qquad M_6 = \pm (n-2)^{n-2} a_1{}^2 a_2{}^{n-1} a_n{}^{n-3},$$
$$M_7 = \pm 2^2 (n-2)^{n-2} a_0{}^{n-3} a^n{}_{n-2} a_n, \quad M_8 = \pm 3^3 (n-3)^{n-3} a_0{}^2 a_3{}^n a_n{}^{n-4},$$
$$M_9 = \pm 2^2 (n-3)^{n-3} a_1{}^{n-2} a_{n-2}^{n-1} a_n .$$

Le suddivisioni della presente dimostrazione dipendenti dal modulo k sono elencate qui sotto con i monomi usati in ciascun caso

(I)	$k+(n-1)^{n-1}$,	$k+n^n$	M_1, M_2
(II)	$k \mid n^n$,	$k \neq 2^q$	M_1, M_3, M_4, M_7
(III)	$k \mid n^n$,	$k=2^q$, $2<q$	M_1, M_4, M_8, M_9
(IV)	$k \mid (n-1)^{n-1}$,	$k+4$	M_2, M_3, M_5, M_6, M_7 e, se n è pari, M_9.

Questi quattro casi includono tutte le possibili eventualità. Ciascuno dei monomi elencati compare con coefficiente non nullo sotto le supposte condizioni per k. Useremo inoltre r_j, s_j, t_j, per indicare rispettivamente gli esponenti del primo, secondo e terzo fattore letterale di M_j. Allora, se è $D=PQ$, quando M_1 compare in D esiste in P un termine $a_0^{r_1}a^{s_1}{}_{n-1}$. Simili osservazioni possono essere fatte per ciascun M_j ($j=1,\ldots,9$). Gli esponenti r_j, s_j, t_j sono interi non negativi al massimo eguali ai corrispondenti esponenti di M_j. Come nel caso di $R(f, g)$ la dimostrazione della irriducibilità di $D(\mathrm{mod}\, k)$ dove $k+4$ sarà basata sul fatto che ciascun fattore P, Q è omogeneo e isobarico. Inoltre, poichè o M_3 o M_4 è sempre presente, ciascun fattore di grado positivo deve avere peso positivo.

4. *Irriducibilità del discriminante.* Supponiamo che sia $D=PQ$ dove P e Q sono di grado positivo e dimostriamo che questa ipotesi porta a contradizioni in ciascuno dei quattro casi elencati sopra.

Se M_1 e M_2 sono presenti, i pesi dei corrispondenti termini in P soddisfano a

$$0 \leq (n-1)s_1 = ns_2 < n(n-1), \qquad s_1 \leq n.$$

Poichè n e $n-1$ sono primi tra loro, il sistema di sopra implica $s_1=n$, $n-1<n-1$.

Se M_1, M_3, M_4 e M_7 sono presenti, abbiamo

$$(n-1)s_1 = r_3+(n-1)s_3 = r_4+ns_4 = (n-2)s_7+nt_7;$$

in particolare

$$(n-1)s_1 = r_4+s_4+(n-1)s_4;$$

ciò implica che è $r_4+s_4=n-1$, dato che il grado r_4+s_4 è positivo e minore di $2n-2$. Allora, poichè il grado di D è $2n-2$, P e Q hanno ciascuno il grado $n-1$. Il sistema di sopra implica anche che $(n-1) \mid r_3$. Nel fattore nel quale è $r_3>0$ ciò implica

che è $r_3 = n-1$, $s_3 = 0$ (poichè il grado è $n-1$), e il peso del fattore è $n-1$. La presenza di M_7 allora dà un termine di peso $(n-2)s_7 + nt_7 = n-1$, che porta a contradizione per $n > 3$. Se $n = 3$, abbiamo $k \mid 27$, $r_1 = s_1 = 1$, $r_3 = r_4 = 2$, $s_3 = s_4 = 0$ e $PQ = (a_1^2 - 4a_0a_2)(a_2^2 - 4a_1a_3) \mp D = a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 + 18a_0a_1a_2a_3 - 27a_0^2a_3^2$.

Se $k \mid n^n$, $k = 2^q$, $2 < q$, allora M_1, M_4, M_8 e M_9 sono presenti, n è pari, P e Q hanno ciascuno il grado $n-1$ come sopra, e abbiamo

$$r_4 + s_4 = r_9 + s_9 + t_9 = n-1,$$
$$r_4 + ns_4 = r_9 + (n-2)s_9 + nt_9.$$

Questo sistema implica $(n-1)r_4 = (n-1)r_9 + 2s_9$ e poichè n è pari, $(n-1) \mid s_9$. Allora $s_9 = 0$ in un fattore di D e $= n-1$ nell'altro fattore. Consideriamo il fattore nel quale è $s_9 = 0$ e così il grado è $r_9 + t_9 = n-1$ dove $r_9 \leq n-2$ e $t_9 \leq 1$. Ciò implica che è $r_9 = n-2$, $t_9 = 1$, e il peso è $2n-2$. La presenza di M_8 dà il sistema

$$r_8 + s_8 + t_8 = n-1, \qquad 3s_8 + nt_8 = 2n-2$$

che è compatibile solo se è $n = 4$ poichè esso implica $(n-3)t_8 = 3r_8 + 1 - n$ dove $r_8 \leq 2$, $t_8 \leq n-4$, e $4 \leq n$. Se $n = 4$, $k \nmid (n-2)^{n-2}$ e la presenza di M_3 dà $r_3 + s_3 = 3$, $r_3 + 3s_3 = 6$ e quindi $2s_3 = 3$.

Se $k \nmid (n-1)^{n-1}$, $k \nmid 4$, allora M_2, M_3, M_5 e M_6 sono presenti, è $4 \leq n$, e abbiamo

$$0 < r_2 + s_2 = r_3 + s_3 = r_5 + s_5 + t_5 = r_6 + s_6 + t_6,$$
$$0 < ns_2 = r_3 + (n-1)s_3 = 2s_5 + nt_5 = r_6 + 2s_6 + nt_6.$$

Questo sistema implica che $n \mid (r_3 - s_3)$ dove $r_3 \leq n-1$, $s_3 \leq n-1$, e perciò $r_3 = s_3 = s_2 = r_2$. La relazione $ns_2 = 2s_5 + nt_5$ implica che $n \mid 2s_5$. Se n è dispari, allora è $s_5 = 0$ o $s_5 = n$; se $n = 2m$, allora è $s_5 = 0$, m o n. I casi $s_5 = 0$ e $s_5 = n$ sono equivalenti, e considereremo il fattore nel quale è $s_5 = 0$. La relazione $nr_2 = nr_5 + (n-2)s_5$, ottenuta dal sistema di sopra, implica allora $r_2 = r_5$ dove $r_5 \leq 1$. $0 < ns_2$ implica $s_2 = r_2 = r_5 \neq 0$. Perciò $r_2 = r_5 = 1$, $-r_2 + (n-1)s_2 = s_6 + (n-1)t_6$, $(n-1) \mid (s_6 + 1)$. Allora $s_6 = n-2$, $1 + t_5 = r_6 + (n-2) + t_6$, $nt_5 = r_6 + 2(n-2) + nt_6$, e $n = (n-1)r_6 + (n-2)^2$, che porta contradizione per $n > 4$. Se $n = 4$, abbiamo $k \mid 27$, $r_5 = t_5 = 1$, $s_5 = r_6 = t_6 = 0$, $s_6 = 2$, nel qual caso un fattore di D contiene a_0a_4 e a_2^2, l'altro fattore contiene a_2^4 e $a_1^2a_2a_4$, e D contiene a_2^6, il che è impossibile perchè a_2 non compare nè nelle prime due colonne nè nell'ultima delle sette colonne del determinante D_4.

Se n è pari, sia $n = 2m$ e si abbia $s_5 = m$, sotto le condizioni di sopra per k. Allora M_2, M_5, M_7 e M_9 sono presenti e abbiamo

$$r_2 + s_2 = r_5 + s_5 + t_5 = r_7 + s_7 + t_7,$$
$$ns_2 = 2s_5 + nt_5 = (n-2)s_7 + nt_7.$$

La relazione $nr_2 = nr_7 + 2s_7$ ottenuta da questo sistema implica che $n \mid 2s_7$, quindi $s_7 = 0$, o m, o n. Inoltre, le condizioni $s_7 = 0$ e $s_7 = n$ sono equivalenti come nel caso di s_5 trattato sopra, e di più nel fattore per il quale è $s_7 = 0$ si ottiene un sistema di equazioni tra gli esponenti equivalente a quello ottenuto quando $s_5 = 0$. In conseguenza occorre considerare soltanto il caso $s_5 = s_7 = m$. In tal caso è $2ms_2 = (2m-2)m + 2mt_7$ onde $s_2 = (m-1) + t_7$, dove $t_7 \leq 1$. Se $t_7 = 1$, è $s_2 = m$, il grado è $2m$ e il peso mn. La presenza di M_9 allora dà

$$r_9 + s_9 + t_9 = 2m,$$
$$r_9 + (2m-2)s_9 + 2mt_9 = 2m^2,$$

e questo sistema implica

$$(2m-3)s_9 + (2m-1)t_9 = 2m^2 - 2m$$

dove $t_9 \leq 1$. Perciò è $(2m-3)s_9 = m(2m-3) + b$, dove $b = m$ se $t_9 = 0$, $b = 1 - m$ se $t_9 = 1$, e in ambo i casi una contradizione è ottenuta se $n \neq 4$. Se $t_7 = 0$, è $s_2 = m - 1$, il grado è $2m - 2$, il peso è $2m(m-1)$, e la presenza di M_9 implica $(2m-3)s_9 + (2m-1)t_9 = (2m-2)(m-1)$ dove $t_9 \leq 1$. Allora è

$$(2m-3)s_9 = m(2m-3) - m + 2 \quad \text{se} \quad t_9 = 0$$
$$(2m-3)s_9 = (m-1)(2m-3) - m \quad \text{se} \quad t_9 = 1,$$

e in ambo i casi una contradizione è ottenuta, se $n \neq 4$. Se $n = 4$ in ciascuno dei due casi di sopra vi è un fattore di D di grado 4 e peso 8, l'altro fattore di grado 2 e peso 4. Questo è precisamente il caso che è stato dimostrato poco sopra condurre a contradizione.

5. *Fattorizzazione di* D *modulo* 2 *e* 4. Per $k = 2$ poniamo $g \equiv f + xf' \pmod 2$ e $h \equiv f' \pmod 2$. Allora g ed h sono ambedue polinomi in x^2, la prima colonna di $R(f + xf', f')$ ha $(1+n)a_0$ e na_0 come suoi elementi non necessariamente nulli per ogni n, ed è

$$D = \frac{1}{a_0} R(f, f') = \frac{1}{a_0} R(f + xf', f') \equiv R(g, h) \pmod 2.$$

Si noti che uno ed uno solo dei polinomi g, h ha grado minore di quello di f, f' rispettivamente. Se in due polinomi g, h con

coefficienti complessi mancano i termini di grado dispari, è stato dimostrato [4] che l'eliminante $E(g, h)$ per la indeterminata x e l'eliminante $E^*(g, h)$ per la indeterminata x^2 soddisfano alla relazione

$$E = cE^{*2}$$

dove c è un numero complesso. Questa identità rimane se i coefficienti dei termini di grado pari in g, h sono delle indeterminate e, applicando al caso nostro, abbiamo

$$R = cR^{*2}.$$

R^* è irriducibile per il n° 2 di questo lavoro. Se è $n = 2p$, g ha il grado p in x^2, h ha il grado $p-1$, e (dal n° 2) $R^*(g, h)$ contiene un termine $[(2p+1)a_0]^{p-1}a^p{}_{2p-1}$ con coefficiente di valore numerico 1. Allora R^{*2} contiene un termine congruo a $M_1 \pmod 2$ (v. n° 3). Similmente se $n = 2p+1$, g ha il grado p in x^2, h ha il grado p, R^* contiene $\pm[(2p+1)a_0]^p a_n{}^p$, e R^{*2} contiene $M_2 \pmod 2$. Perciò per ogni intero positivo n abbiamo

$$D \equiv R^{*2} \pmod 2$$

dove R^* è un polinomio irriducibile (5).

Per $k = 4$ osserviamo che ogni polinomio $f(x)$ con coefficiente iniziale a_0 e con i coefficienti nel campo dei numeri complessi ha il discriminante

$$D = a_0{}^{2n-2} \prod_{i<j} (x_i - x_j)^2$$

dove le x_j sono le radici di f [2; 110]. Nell'anello di polinomi $I[x_1, x_2, \ldots, x_n]$, dove I è l'anello degli interi, è

$$(x_i - x_j)^2 \equiv (x_i + x_j)^2 \pmod 4$$

e quindi

$$D \equiv [a_0{}^{n-1} \prod_{i<j} (x_i + x_j)]^2 \equiv P^2 \pmod 4.$$

(5) [*Nota della Redazione*]. La formula $R = R^{*2}$ (dunque con $c = 1$), dove R è il risultante (nella forma di SYLVESTER adoperata dall'A.) di due polinomi qualisivogliano in x^2, $g(x^2)$, $h(x^2)$, ed R^* quello di $g(x)$, $h(x)$, può dimostrarsi per via del tutto elementare. Basta permutare in R le righe e le colonne mettendo (ordinatamente) prima quelle di ordine dispari e poi quelle di ordine pari; si ottiene

$$R = \begin{vmatrix} R^*, & 0 \\ 0, & R^* \end{vmatrix},$$

dove i simboli 0 rappresentano opportune matrici nulle.

P è un polinomio nei coefficienti di f poichè esso è simmetrico nelle radici di f, e a_0 non divide D (n° 3). Perciò nel campo complesso abbiamo l'identità

$$D = P^2 + 4T$$

dove P e T sono polinomi nei coefficienti di f con coefficienti interi. Questa identità rimane se i coefficienti di f sono delle indeterminate.

Finalmente paragoniamo il risultato ora ottenuto mod 4 con quello ottenuto precedentemente mod 2, e osserviamo che

$$P^2 \equiv R^{*2} \pmod 2$$

implica non solamente

$$P \equiv R^* \pmod 2$$

ma anche

$$P^2 \equiv R^{*2} \pmod 4.$$

Perciò è $D \equiv R^{*2} \pmod 2$ e $D \equiv R^{*2} \pmod 4$.

BIBLIOGRAFIA

[1] ALDO ANDREOTTI, *Sul risultante di due polinomi* « Bollettino della Unione Matematica Italiana », serie 3 vol. 4 (1949), pp. 168-169.

[2] ROBERT FRICKE, *Lehrbuch der Algebra*, vol. 1, Braunschweig, 1924.

[3] F. S. MACAULAY, *The Algebraic Theory of Modular Systems*, Cambridge Tracts in Mathematics and Mathematical Physics, No. 19, Cambridge, 1916.

[4] J. M. THOMAS, *Eliminants*, « American Journal of Mathematics », vol. 69 (1947), pp. 592-598.