Bollettino
Unione Matematica Italiana

Vincenzo Amato

# Le curve algebriche nella teoria delle equazioni secondo Galois

*Bollettino dell'Unione Matematica Italiana, Serie 3*, Vol. **4** (1949), n.2, p. 104–109.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1949_3_4_2_104_0>

# Le curve algebriche nella teoria delle equazioni secondo Galois.

Nota di VINCENZO AMATO (a Catania).

**Sunto.** - *Si espone una veduta d'insieme delle possibilità di abbassamento del gruppo algebrico di una curva algebrica (che può essere approfondita nella rappresentazione reale sulla Riemanniana) col solo ausilio della nozione di sottogruppo fondamentale del totale.*

**1.** Chiameremo *curva algebrica r.pla a gruppo ciclico* una curva

$$\alpha_0(z)u^r + \alpha_1(z)u^{r-1} + \ldots + \alpha_r(z) = 0, \tag{1}$$

con le $\alpha$ funzioni razionali intere di $z$, il cui gruppo algebrico (cioè il gruppo di GALOIS nel campo $R$ dei coefficienti delle $\alpha$ ampliato con la $z$) sia quello delle $r$ potenze del ciclo $(u_1 u_2 \ldots u_r)$ sulle radici $u_1, u_2, \ldots u_r$.

Se si aggiunge al campo $R$ una radice della (1), il gruppo algebrico si abbassa a quel sottogruppo di esso che la lascia ferma e perciò, nel nostro caso, a quello che lascia ferme tutte le radici cioè all'identità.

Ogni curva algebrica a gruppo ciclico, in conseguenza di ciò, è tale che per una sua radice qualunque, ad esempio $u_1$, si ha:

$$u_2 = \Theta(u_1),\ u_3 = \Theta(u_2) = \Theta(\Theta(u_1)), \ldots$$

essendo $\Theta$ una funzione razionale.

Se si pone per brevità:

$$\Theta(\Theta(u_1)) = \Theta^{(2)}(u_1),\ \Theta(\Theta^{(2)}(u_1)) = \Theta^{(3)}(u_1), \ldots$$

si può scrivere:

$$u_2 = \Theta(u_1),\ u_3 = \Theta^{(2)}(u_1), \ldots, u_r = \Theta^{(r-1)}(u_1)$$

ottenendo infine:

$$\Theta^{(r)}(u_1) = u_1 .$$

Se la (1) è irriducibile nel campo di tutte le costanti, il suo gruppo di monodromia, dovendo essere transitivo (1), coincide col gruppo algebrico.

(1) ENRIQUES e CHISINI: *Lezioni sulla teoria geometrica delle equazioni e delle funzioni algebriche*, Bologna, Zanichelli, Vol I, libro 2°, pag. 350, o L. BIANCHI: *Lezioni sulla teoria dei gruppi di sostituzioni e delle equazioni algebriche secondo* GALOIS, Pisa, Spoerri, 1900, pag. 238.

Indichiamo con $\mu_i$ il numero degli eventuali punti di diramazione intorno a ciascuno dei quali si realizzi la $S^{h_i}$, essendo $h_i$ primo con $r$ e minore di $r$, e perciò $i = 1, 2, \dots, \varphi(r)$; con $\nu_j$ quello dei punti di diramazione (eventuali) relativi alla $S^{\delta_j}$, essendo $\delta_j$ divisore di $r$ diverso da 1 e da $r$, e perciò $j = 1, 2, \dots, N(r)$, se $N(r)$ è il numero di tali divisori; con $\rho_l$ il numero degli eventuali punti di diramazione relativi alla $S^{k_l}$, essendo $k_l$ minore di $r$, non divisore di $r$, e non primo con $r$, e perciò: $l = 1, 2, \dots, \lambda(r)$, se $\lambda(r)$ sono i numeri $k_l$.

Se $q$ è il numero complessivo dei punti di diramazione, risulterà:

$$\sum_{i=1}^{\varphi(r)} \mu_i + \sum_{j=1}^{N(r)} \nu_j + \sum_{l=1}^{\lambda(r)} \rho_l = q,$$

$$\varphi(r) + N(r) + \lambda(r) = r - 1.$$

Applicando una formula generale di RIEMANN [2] e indicando con $D_l$ il massimo comun divisore dei numeri $r$ e $k_l$ (quando sia $k_l$ non nullo), si ha facilmente:

$$2p = (r-1)(q-2) - \sum_{j=1}^{N(r)} (\delta_j - 1)\nu_j - \sum_{l=1}^{\lambda(r)} (D_l - 1)\rho_l .$$

In questa relazione, fissato ogni volta il *genere* $p$, si possono fare le varie ipotesi: $q = 2, 3, \dots$ e risolvere l'equazione che ne risulta per valori nulli o interi positivi delle $\mu_i, \nu_j, \rho_l$, tenendo presente che un cammino chiuso avvolgente tutti i punti di diramazione produce la sostituzione identica.

Se $r$ è primo si ha:

$$2p = (r-1)(q-2).$$

**2.** Premesso ciò, consideriamo una curva algebrica

$$\alpha_0(z)u^m + \alpha_1(z)u^{m-1} + \dots + \alpha_m(z) = 0 \tag{2}$$

e supponiamo che, nel campo $R$ di razionalità dei coefficienti delle $\alpha$ ampliato con $z$, il gruppo di GALOIS della (2) sia il gruppo di tutte le sostituzioni del totale su $m = \rho r$ lettere permutabili con la sostituzione

$$S = (u_1 \dots u_r)(u_{r+1} \dots u_{2r}) \dots (u_{(\rho-1)r+1} \dots u_m), \tag{3}$$

cioè sia il gruppo $G_S$, d'ordine $\rho! r^\rho$, detto *sottogruppo fondamentale del totale* (sulle $u_1, \dots, u_m$), del quale è nota la struttura [3].

[2] APPELL *et* GOURSAT: *Théorie des fonctions algébriques et de leurs intégrales*, Paris, Gauthier - Villars, 1895, pag. 233.

[3] V. AMATO: *Sul gruppo totale di sostituzioni su* n *lettere*, «Atti Acc. Gioenia», Catania, serie 5ª, Vol. XX, 1934.

Ogni gruppo $G_S$ è imprimitivo e le $m$ lettere sulle quali opera si possono ripartire nei $\rho$ sistemi di imprimitività:

$$(4) \qquad u_1 \dots u_r, u_{r+1} \dots u_{2r}, \dots, u_{(\rho-1)r+1} \dots u_m,$$

contenenti ciascuno $r$ lettere, tali che ogni sostituzione di $G_S$ o fa ruotare le lettere di un sistema nel sistema stesso permutandole ciclicamente o le porta tutte in quelle di un altro nell'ordine in cui queste ultime sono scritte o permutate ciclicamente.

Si considerino ora i sistemi:

$$(5) \qquad u_{i_1} \dots u_{i_\rho}, u_{j_1} \dots u_{j_\rho}, \dots$$

contenenti ciascuno $\rho$ lettere scelte rispettivamente nei sistemi (4) in un modo qualsiasi.

Ad esempio. se $\rho = r = 2$ e perciò

$$S = (u_1u_2)(u_3u_4),$$

il gruppo $G_S$ è il seguente:

$$1, (u_1u_3u_2u_4), (u_1u_2)(u_3u_4), (u_1u_4u_2u_3)$$
$$(u_1u_2), (u_3u_4), (u_1u_3)(u_2u_4), (u_1u_4)(u_2u_3);$$

i sistemi d'imprimitività sono:

$$u_1u_2, u_3u_4$$

e gli altri sistemi da considerarsi sono:

$$u_1u_3, u_1u_4, u_2u_3, u_2u_4,$$
$$u_3u_1, u_4u_1, u_3u_2, u_4u_2.$$

Se si prende uno dei sistemi (5), ad esempio:

$$u_{i_1}u_{i_2} \dots u_{i_\rho},$$

si ha, in applicazione di una proposizione generale richiamata al principio dell'art. 1, che, ampliando il campo $R$ con l'aggiunta delle $u_{i_1}, u_{i_2}, \dots, u_{i_\rho}$, il gruppo di GALOIS della (2) si abbassa all'identità e quindi si ha:

$$u_i = f_i(u_{i_1}, \dots, u_{i_\rho}),$$

essendo $f_i$ funzione razionale, in $R$, delle $u_{i_1}, \dots, u_{i_\rho}$.

V. AMATO: *Sul gruppo di monodromia delle equazioni a gruppo algebrico* $G_S$, «Bollettino dell'U.M.I., 1948, fasc. 3°.

V. AMATO: *Sulle equazioni algebriche il cui gruppo di* GALOIS *è un sottogruppo fondamentale del totale*, «Rendiconti del Circolo mat. di Palermo», Tomo LVIII, 1934.

Se a queste ultime si sostituiscono, ad esempio, le $u_{j_1}, \dots, u_{j_\rho}$ di un altro sistema (5), si hanno le seguenti condizioni di permutabilità necessarie e sufficienti perchè la (2) sia a gruppo $G_S$:

$$(6)\qquad \begin{aligned} f_{j_1}(f_{i_1+1}, \dots, f_{i_\rho+1}) &= f_{i_1+1}(f_{j_1}, \dots, f_{j_\rho}), \\ f_{j_2}(f_{i_1+1}, \dots, f_{i_\rho+1}) &= f_{i_2+1}(f_{j_1}, \dots, f_{j_\rho}), \\ &\dots\dots\dots\dots\dots\dots\dots \\ f_{j_\rho}(f_{i_1+1}, \dots, f_{j_\rho+1}) &= f_{i_\rho+1}(f_{j_1}, \dots, f_{j_\rho}). \end{aligned}$$

intendendo che se, per semplicità, gl'indici $i_1 + 1$, $i_2 + 1, \dots, i_\rho + 1$ sono supposti in ordine crescente, debbano essere sostituiti con $1, r + 1, \dots, (\rho - 1)r + 1$, quando sia rispettivamente $i_1 = r, i_2 = 2r, \dots, i_\rho = \rho r$ e che le $f$ dentro parentesi siano tutte funzioni delle $u_{i_1}, u_{i_2}, \dots, u_{i_\rho}$[4].

Si può perciò concludere, includendo i risultati dell'art. 1, che:

*Le* m *radici della* (2) *sono funzioni razionali di* $\rho$ *di esse, costituenti uno stesso sistema* (5), *e queste funzioni razionali sono legate dalle* (6).

**3.** Il gruppo algebrico $G_S$ della (2), quando si ponga:

$$y_1 = (a - u_1) \dots (a - u_r),$$

essendo $a$ un numero di $R$, e si aggiunga al campo la $y_1$, si abbassa al suo sottogruppo che lascia fermo il sistema $u_1 u_2 \dots u_r$ nel senso che ne fa circolare le lettere nel sistema stesso.

Nel nuovo campo di razionalità si avrà perciò:

$$(u - u_1) \dots (u - u_r) = u^r + \beta_1(z, y_1)u^{r-1} + \dots + \beta_r(z, y_1),$$

essendo le $\beta$ funzioni razionali delle $z$, $y_1$ coi coefficienti in $R$.

Se si pone ancora:

$$\begin{aligned} y_2 &= (a - u_{r+1}) \dots (a - u_{2r}), \\ &\dots\dots\dots\dots\dots\dots \\ y_\rho &= (a - u_{(\rho-1)r+1}) \dots (a - u_m) \end{aligned}$$

e si sceglie il numero $a$ di $R$ in modo che $y_1, y_2, \dots, y_\rho$ siano numericamente distinti, si ha la risolvente:

$$\varphi(z, y) = (y - y_1)(y - y_2) \dots (y - y_\rho) = 0$$

e si ottiene:

$$f(z,u) = \alpha_0(u - u_1) \dots (u - u_m) = \alpha_0 \prod_{i=1}^{i=\rho} [u^r + \beta_1(z, y_i)u^{r-1} + \dots + \beta_r(z, y_i)] = 0.$$

(4) V. AMATO: «Memoria del Circolo mat. di Palermo», richiamata in (3).

Si perviene perciò a questo risultato:

*L'equazione della curva algebrica data, irriducibile e a gruppo algebrico* $G_S$, *risulta dall'eliminazione della* y *fra le equazioni:*

$$\varphi(z, y) = 0,$$
$$u^r + \beta_1(z, y)u^{r-1} + \ldots + \beta_r(z, y) = 0.$$

*I gruppi di* GALOIS *delle equazioni;*

$$u^r + \beta_1(z, y_i)u^{r-1} + \ldots + \beta_r(z, y_i) = 0,$$
$$(i = 1,2, \ldots, \rho),$$

*sono ciclici e simili fra loro.*

Si può ancora dire, collegando i risultati ottenuti con quelli dell'art. 1, che se la (2) è irriducibile nel campo di tutte le costanti, le sue singolarità derivano da quelle della $u$ definita dall'equazione

$$u^r + \beta_1(z, y)u^{r-1} + \ldots + \beta_r(z, y) = 0$$

ciclica sulla riemanniana della curva

$$\varphi(z, y) = 0.$$

**4.** Consideriamo ora l'equazione *generale* di grado $m$ nella $u$:

$$f(z,u) = 0 \tag{7}$$

di una curva algebrica.

Il gruppo (algebrico) della (7), nel campo $R$ dei coefficienti ampliato con la $z$, è il gruppo totale $G_{m!}$ su $m$ lettere e non si abbassa ad un suo sottogruppo ampliando il campo con costanti determinate [5].

Se $m = \rho r$, posto

$$S = (u_1 \ldots u_r)(u_{r+1} \ldots u_{2r}) \ldots (u_{(\rho-1)r+1} \ldots u_m),$$

indicando con $\varepsilon$ una radice primitiva $r^{ma}$ dell'unità, si dimostra facilmente [6] che, ampliando il campo $R$ con l'aggiunta di $\varepsilon$ e dell'irrazionalità:

$$\xi_1 = (u_1 + \varepsilon u_2 + \ldots + \varepsilon^{r-1}u_r)^r + \ldots + (u_{(\rho-1)r+1} + \varepsilon u_{(\rho-1)r+2} + \ldots + \varepsilon^{r-1}u_m)^r,$$

il gruppo $G_{m!}$ si abbassa al suo sottogruppo fondamentale $G_S$.

[5] MILLER, BLICHFELDT e DICKSON: *Theory and applications of finite groups*, New York, J. Wiley, 1916, pag. 295.

[6] V. AMATO: *L'equazione generale di grado* n *considerata nel campo ampliato di razionalità nel quale diventa a gruppo* $G_S$, «Atti dell'Acc. Gioenia», Catania, serie 6ª, Vol. III, 1937.

La risolvente che ne risulta

$$(\xi - \xi_1)(\xi - \xi_2) \dots (\xi - \xi_k) = 0, \qquad \left(k = \frac{m!}{\rho! r_\rho}\right),$$

ha per gruppo di GALOIS il gruppo

$$\frac{G_{m!}}{G_S}$$

in isomorfismo con $G_{m!}$.

Questo isomorfismo è oloedrico per $m > 4$ [7].