ATTI

DELLA

REALE ACCADEMIA DEI LINCEI

ANNO CCCXV.

1918

SERIE QUINTA

RENDICONTI

Classe di scienze fisiche, matematiche e naturali.

VOLUME XXVII.

1° SEMESTRE.

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA DEI LINCEI

PROPRIETÀ DEL DOTT. PIO BEFANI

1918

Matematica. — *Proprietà caratteristiche delle equazioni di grado primo p risolubili per radicali.* Nota del dott. Giulio Darbi, presentata dal Socio L. Bianchi.

Con la presente Nota, che ha lo scopo di determinare un nuovo criterio per riconoscere se un'equazione di grado primo p è risolubile per radicali [1], dimostreremo il seguente teorema:

La condizione necessaria e sufficiente affinchè un'equazione di grado primo p, irriducibile nel campo assoluto (C) di razionalità, a cui appartengono i suoi coefficienti, sia risolubile per radicali, è che qualunque funzione razionale in (C) [2] delle sue radici si possa esprimere in funzione lineare omogenea di $(p-1)$ radici, con coefficienti che sono funzioni razionali in (C) della rimanente radice.

1. Sia:

$$f(x)=0 \tag{1}$$

un'equazione di grado primo p, irriducibile nel campo assoluto (C) di razionalità, a cui appartengono i suoi coefficienti, la quale sia risolubile per radicali. Sappiamo che il suo gruppo (G) di Galois è d'ordine $p\delta$, essendo δ un divisore di $(p-1)$. Esaminiamo dapprima il caso in cui sia δ uguale a $(p-1)$. Denotando con $x_0, x_1, \ldots, x_{p-1}$ le radici della (1), sappiamo che tutto il gruppo metaciclico si genera con le due sostituzioni elementari

$$S=(x_0, x_1, \ldots, x_{p-1}) \quad , \quad T=(x_1, x_g, \ldots, x_{g^{p-2}})\,;$$

le sue $p(p-1)$ sostituzioni sono date dalla formola

$$U=S^\beta T^\alpha \begin{cases} \alpha=0,1,2,\ldots,p-2 \\ \beta=0,1,2,\ldots,p-1\,. \end{cases}$$

Aggiungendo al campo (C) la radice x_0, il gruppo (C) si ridurrà al gruppo ciclico formato da T e dalle potenze $T^2, T^3, \ldots, T^{p-1}=1$, mentre l'equazione data (1) si riduce all'equazione abeliana a gruppo ciclico:

$$\frac{f(x)}{x-x_0}=0\,, \tag{2}$$

di grado $(p-1)$, irriducibile nel campo $(C\,;x_0)$.

[1] Cfr. Luigi Bianchi, *Teoria dei gruppi di sostituzioni e delle equazioni algebriche secondo Galois*, an. 1899, pp. 197-200, edit. Spoerri, Pisa.

[2] Con l'espressione: funzione razionale in (C) delle radici, intendiamo dire: funzione razionale delle radici con coefficienti appartenenti a (C)

Ricordiamo il seguente teorema [1]:

La condizione necessaria e sufficiente, affinchè un'equazione ciclica di grado n, irriducibile in un certo campo (K) di razionalità, a cui appartengono i suoi coefficienti, goda della proprietà per cui: ogni funzione razionale in (K) delle sue radici si possa esprimere in funzione lineare di queste con coefficienti appartenenti a (K), è che fra le radici $x_1, x_2, \ldots, x_n$ della data equazione non esista alcuna relazione del tipo:

$$x_1 + x_2 + \cdots + x_d = C, \tag{3}$$

essendo C un numero di (K); d un divisore di n; $d < n$.

Giova notare che il precedente teorema sussiste, se nel campo (K) sono irriducibili le equazioni che danno le radici primitive t^{me} dell'unità, essendo t un divisore di n uguale o minore di n.

Dimostreremo che le menzionate condizioni sono soddisfatte dall'equazione (2). Sappiamo che le radici primitive t^{me} dell'unità, essendo t un divisore di $(p-1)$ soddisfano ad un'equazione abeliana [2]:

$$\psi(\varepsilon) = 0, \tag{4}$$

di grado $\lambda < t$, irriducibile in (C). Se la (4) fosse riducibile nel campo (C, x_0), il suo gruppo (H) d'ordine λ, dovrebbe ridursi ad un suo sottogruppo (H_1) d'indice p in (H) [2]; ciò è impossibile, essendo tale indice minore di p.

Se fra le radici della (2) esistesse una relazione del tipo (3), essendo c un numero del campo (C, x_0), d un divisore di $(p-1)$; $d < p-1$, applicando alla (3) le sostituzioni $T, T^2, T^{p-1} = 1$, e sommando le relazioni ottenute, si avrebbe:

$$d \sum_{i=1}^{i=p-1} x_i = c(p-1). \tag{5}$$

Denotando con q il coefficiente del 2° termine dell'equazione data (1), dalla (5) si ricaverebbe:

$$c = -\frac{d(q + x_0)}{p-1}.$$

Sostituendo nella (3) al numero c l'espressione che figura nel 2° membro della (5), si ottiene:

$$(p-1)(x_1 + x_2 + \cdots + x_d) + dx_0 = -dq. \tag{6}$$

È facile dimostrare che una relazione del tipo (6) fra le radici della (1)

[1] Cfr. Annali di Matematica pura ed applicata, *Sulle equazioni abeliane a gruppo ciclico*, 1917.

[2] Cfr. Bianchi, op. cit., pp. 189, 207, 212.

con coefficienti appartenenti a (C), non può sussistere. Applicando alla (6) le sostituzioni $S, S^2, \dots, S^{p-1} = 1$, si ottiene un sistema di p equazioni lineari nelle radici $x_0, x_1, \dots, x_{p-1}$. Il determinante D fra i coefficienti è un circolante d'ordine p; sappiamo [1] che è uguale al prodotto

$$(-1)^{\frac{(p-1)(p-2)}{2}} \varphi(\varepsilon_0)\, \varphi(\varepsilon_1) \dots \varphi(\varepsilon_{p-1}),$$

essendo:

$$\varphi(\varepsilon_i) = d + (p-1)(\varepsilon_i + \varepsilon_i^2 + \cdots + \varepsilon_i^d),$$

ove $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{p-1}$ sono radici dell'equazione:

$$\varepsilon^p - 1 = 0.$$

Il determinante D è diverso da zero, perchè nessuno dei polinomi $\varphi(\varepsilon_0), \varphi(\varepsilon_1), \dots, \varphi(\varepsilon_{p-1})$ è nullo, tenuto conto che l'equazione:

$$\varepsilon^{p-1} + \varepsilon^{p-2} + \cdots + \varepsilon + 1 = 0$$

è irriducibile in (C).

Onde, risolvendo il menzionato sistema rispetto alle incognite $x_0, x_1, \dots, x_{p-1}$, queste, che sono radici dell'equazione (1), avrebbero valori appartenenti a (C); il che è assurdo, avendo supposto che l'equazione (1) sia irriducibile in (C).

Applicando all'equazione (2) il teorema, citato al principio di questo articolo, si conclude che:

ogni funzione razionale in (C) delle radici $x_0, x_1, \dots, x_{p-1}$ si può esprimere in funzione lineare omogenea di $x_1, x_2, \dots, x_{p-1}$ con coefficienti appartenenti al campo $(C; x_0)$.

Al precedente risultato siamo pervenuti, avendo supposto che l'equazione (1) abbia per gruppo di Galois il metaciclico. Se il gruppo della (1) fosse un sottogruppo del metaciclico, il suo ordine sarebbe uguale a ph, essendo h un divisore di $(p-1)$. Seguendo lo stesso ragionamento, tenuto nelle pagine precedenti, si arriverebbe al seguente risultato:

ogni funzione razionale in (C) delle radici della (1), si può esprimere in funzione lineare omogenea di h radici, con coefficienti appartenenti al campo $(C; x_0)$, essendo h un divisore di $p-1$.

2. Dimostriamo l'inverso del teorema ora enunciato, cioè:

se ogni funzione razionale delle radici di un'equazione di grado primo p, irriducibile nel campo assoluto (C) di razionalità, si può esprimere in funzione lineare omogenea di $(p-1)$ radici, con coefficienti che sono funzioni razionali in (C) dell'altra radice, l'equazione data è risolubile per radicali.

Supponiamo che l'equazione:

$$f(x) = 0 \tag{7}$$

[1] Cfr. Capelli, *Istituzioni d'analisi algebrica*, 1902, pag. 626.

di grado primo p, sia irriducibile nel campo (C) e goda della proprietà testè enunciata. Sappiamo [1] che l'ordine λ del suo gruppo (Γ) è uguale ad un multiplo del grado p, cioè

$$\lambda = pm. \tag{7'}$$

Aggiungendo al campo (C) la radice x_0, il gruppo (Γ) si abbassa ad un suo sottogruppo d'ordine m, le cui sostituzioni lasciano ferma la radice x_0. Se m non è minore di $(p - 1)$, l'equazione:

$$\frac{f(x)}{x - x_0} = 0, \tag{8}$$

di grado $(p - 1)$ in x, avendo il suo gruppo transitivo, è irriducibile nel campo $(C ; x_0)$.

Ricordiamo il seguente teorema [2]:

Se un'equazione, irriducibile in un certo campo (K) di razionalità, a cui appartengono i suoi coefficienti, gode della proprietà, che ogni funzione razionale in (K) delle sue radici si esprime in funzione lineare di queste con coefficienti appartenenti a (K), l'equazione è normale, e quindi l'ordine del suo gruppo è uguale al grado dell'equazione.

Applicando il menzionato teorema alla (8), si ricava che $m = p - 1$. Dalla (7)' si ha:

$$\lambda = p(p - 1),$$

ossia il gruppo della (8) è il metaciclico; quindi la (8) è risolubile per radicali. Se poi $m < p - 1$ è facile dimostrare che il gruppo della (8) coincide con un sottogruppo del metaciclico. Omettiamo tale dimostrazione, che trovasi nell'opera citata del prof. Bianchi a pag. 198.

3. Riassumendo i risultati fin qui ottenuti, possiamo enunciare il seguente teorema:

La condizione necessaria e sufficiente affinchè un'equazione di grado primo p, irriducibile nel campo assoluto (C) *di razionalità, a cui appartengono i suoi coefficienti, sia risolubile per radicali, è che ogni funzione razionale in* (C) *delle sue radici si possa esprimere in funzione lineare omogenea di* $(p - 1)$ *radici, con coefficienti che sono funzioni razionali in* (C) *della rimanente radice.*

[1] Cfr. Bianchi, op. cit., pag. 153.

[2] Cfr. Giornale di Matematiche di Battaglini, 1901.