ATTI

DELLA

REALE ACCADEMIA NAZIONALE DEI LINCEI

ANNO CCCXX

1923

SERIE QUINTA

RENDICONTI

Classe di scienze fisiche, matematiche e naturali.

VOLUME XXXII.

1° Semestre.

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA NAZIONALE DEI LINCEI

PROPRIETÀ DEL DOTT. PIO BEFANI

1923

RENDICONTI

DELLE SEDUTE

DELLA REALE ACCADEMIA NAZIONALE DEI LINCEI

Classe di scienze fisiche, matematiche e naturali.

Seduta del 4 febbraio 1923.

V. VOLTERRA, Vicepresidente.

MEMORIE E NOTE DI SOCI

Matematica. — *Sulla composizione degli ideali primarii assoluti in un corpo algebrico.* Nota del Socio LUIGI BIANCHI.

1. — Riprendo a trattare in questa Nota un argomento di cui mi occupai recentemente in altro scritto (1). Ivi sono partito dal problema di costruire la base per un ideale della specie, assegnata che ne sia la norma, e dalla sua risoluzione ho dedotto le proprietà principali di questi ideali. Qui seguirò una via in certo modo inversa, che muove dalla definizione stessa di ideale primario assoluto per stabilirne le proprietà ed arrivare alla costruzione della base.

Ricordiamo le definizioni:

Un ideale in un corpo algebrico $k(\theta)$ è primario assoluto quando il più piccolo intero razionale, contenuto nell'ideale, coincide colla norma di questo.

Trasformiamo questa definizione in un'altra mediante il seguente teorema, che esprime una proprietà caratteristica di questi ideali:

I) *Un ideale* A *è primario assoluto allora, ed allora soltanto, quando ogni intero del corpo $k(\theta)$ è congruo (mod. A) con un numero intero razionale.*

Per dimostrarlo osserviamo che, se A è un qualunque ideale, ed m indica il minimo numero razionale intero (positivo) contenuto in A, i numeri

(1) *Sugli ideali primarii assoluti in un corpo algebrico.* Journal de mathématiques, 8ème serie, tom. V. (1922).

razionali r in A sono tutti e soli i multipli di m, talchè per due numeri *razionali* r, s in A le due congruenze

$$r \equiv s \pmod{A}$$

ovvero

$$r \equiv s \pmod{m}$$

si equivalgono perfettamente.

Ora supponiamo che qualunque intero in $k(\theta)$ sia congruo (mod. A) con un numero razionale. Per quanto precede, avremo allora in $k(\theta)$ tanti interi incongrui (mod. A) quanti razionali interi esistono incongrui (mod. m). E siccome i primi sono in numero di NA, i secondi in numero di m, sarà

$$NA = m,$$

cioè l'ideale A sarà primario assoluto.

Viceversa, se A è primario assoluto, è $NA = m$, ed m numeri razionali di un sistema completo di resti (mod. m) dànno anche un sistema completo di resti (mod. A). Per ciò, qualunque intero in $k(\theta)$ è congruo (mod. A) con un numero razionale, c. d. d.

2. — Dal teorema I) deriva subito come corollario:

II) *Ogni ideale* B, *divisore di un ideale primario assoluto* A, *è anche primario assoluto.*

Difatti un intero qualunque ω in $k(\theta)$ è congruo (mod. A) con un numero razionale r, e per ciò anche

$$\omega \equiv r \pmod{B},$$

il che prova, secondo I), che B è primario assoluto.

Si osservi che, nelle ipotesi superiori, l'ideale A si risolve nel prodotto di B per un altro ideale C, che sarà, per la ragione stessa, primario assoluto. Ed ora domandiamo inversamente se il prodotto BC di due ideali primarii assoluti sarà anche primario assoluto.

Questo non si può assicurare in generale, come si riscontra sopra semplici esempî (1): ma possiamo dimostrare:

III) *Se le norme* NB, NC *dei due fattori* B, C *primari assoluti sono numeri primi fra loro, anche il prodotto* $A = BC$ *è primario assoluto.*

Difatti, ogni intero ω in $k(\theta)$ è congruo (mod. B) con un numero razionale b, e (mod. C) con un numero razionale c. Siccome NB, NC sono primi fra loro, possiamo prendere un numero razionale a tale che sia

$$a \equiv b \pmod{NB} \quad , \quad a \equiv c \pmod{NC},$$

(1) Così, nel corpo quadratico di numero fondamentale D, ogni numero primo razionale p, tale che D sia residuo quadratico di $4p$, si risolve nel prodotto di due ideali primi P, P′ di 1° grado (eguali o diversi):

$$(p) = P\,P';$$

e, mentre P, P′ sono primarii assoluti, non è tale il prodotto.

ed allora è insieme

$$\omega \equiv a \text{ (mod. B)} \quad , \quad \omega \equiv a \text{ (mod. C)} .$$

Ma gli ideali B, C sono primi fra loro, tali essendo le loro norme, e ne segue

$$\omega \equiv a \text{ (mod. BC)} ,$$

onde BC è primario assoluto.

Il teorema II) si può applicare in particolare ai fattori primi P di A. Ma un ideale primo P contiene, come minimo razionale, il numero primo p a cui è coordinato, ed è quindi primario assoluto solo quando $NP = p$, cioè quando l'ideale primo è di 1° grado; dunque:

IV) *Ogni ideale primario assoluto si decompone in ideali primi, tutti di 1° grado.*

Che la proprietà inversa non sussista in generale, si è già sopra osservato.

3. — I risultati precedenti ci conducono a ricercare se le potenze di un ideale primo P di 1° grado sono ideali primarii assoluti. Per rispondervi stabiliamo il seguente teerema, che vale per ideali primi di qualunque grado:

a) *Se* P *è un ideale primo qualunque, e* p *il suo numero primo razionale coordinato, il minimo numero razionale contenuto in una qualunque potenza* P^r *è dato da* p^r, *eccezione fatta dal caso che* p *sia divisibile per* P^2 (1).

Sia f il grado di P, indi

$$NP = p^f \quad , \quad NP^r = p^{rf} .$$

Il minimo numero razionale contenuto in P^r deve dividere NP^r e sarà dunque una potenza di p, diciamo p^s. Siccome però p^r è in ogni caso contenuto in P^r, sarà p^r divisibile per p^s, cioè $r \geq s$. Se dimostriamo che nello stesso tempo $s \geq r$, sarà provata l'eguaglianza $s = r$, cioè il teorema a). Per questo bisogna tener conto dell'ipotesi che p non è divisibile per P^2 e si ha quindi

$$(p) = PQ ,$$

dove il secondo fattore ideale Q non sarà divisibile per P. E allora la massima potenza di P che entra in

$$(p)^s = P^s Q^s$$

è la P^s. D'altra parte p^s è per ipotesi contenuto in P^r, cioè divisibile per P^r; onde risulta appunto $s \geq r$, c. d. d.

(1) Allora p divide il numero fondamentale D del corpo ed è critico.

Manifestamente il caso escluso (p divisibile per P^2) è in effetto eccezionale, perchè allora il minimo numero razionale contenuto in P^2 è $= p$, e non $= p^2$.

Se applichiamo il teorema *a*) al caso di un ideale primo P di 1° grado, abbiamo il teorema:

V) *Tutte le potenze di un ideale primo* P *di 1° grado sono ideali primarii assoluti, salvo quando p è divisibile per* P^2, *caso in cui la proprietà cessa subito dalla seconda potenza.*

Di qui possiamo dedurre l'esistenza, nel corpo algebrico, di infiniti interi α *primarii assoluti*, cioè tali che il più piccolo numero razionale divisibile per α sia il valore assoluto della norma di α $|N\alpha|$. Si sa infatti che in ogni corpo algebrico esistono infiniti ideali primi di 1° grado non compresi nel caso eccezionale. Se P è un tale ideale, si sa che una potenza convenientemente elevata P^δ di P (dove δ è in ogni caso un divisore del numero h delle classi) dà un ideale principale

$$P^\delta = (\alpha);$$

ed allora, pel teorema V), il numero α è primario assoluto. Si ha dunque come corollario:

In ogni corpo algebrico esistono infiniti numeri interi primarii assoluti.

4. — Trattiamo ora il problema di costruire un ideale primario assoluto A di cui sia assegnata la norma $NA = m$.

Prendiamo una base (minima) del corpo $k(\theta)$ di grado n

$$[\omega_1, \omega_2, \ldots, \omega_n]$$

costituita di n interi, e indichiamo con $c_{ik}^{(l)}$ i numeri razionali interi che dànno le *costanti di composizione* della base, secondo le formole

$$\omega_i \omega_k = \sum_{l=1}^{l=n} c_{ik}^{(l)} \omega_l . \tag{I}$$

Se l'ideale A è primario assoluto, i numeri $\omega_1, \omega_2, \ldots, \omega_n$ della base sono congrui (mod. A) con n numeri razionali interi (n. 1)

$$\xi_1, \xi_2, \ldots, \xi_n,$$

onde le formole (I) si cangiano, pei numeri ξ_i, nelle congruenze quadratiche

$$\xi_i \xi_k \equiv \sum_{l=1}^{l=n} c_{ik}^{(l)} \xi_l \,(\text{mod. A}).$$

Per l'osservazione fondamentale al n. 1, queste congruenze fra numeri razionali (mod. A) equivalgono perfettamente a queste altre rispetto alla norma m dell'ideale A:

$$\xi_i \xi_k \equiv \sum_{l=1}^{l=n} c_{ik}^{(l)} \xi_l \,(\text{mod.}\, m). \tag{II}$$

Ma, oltre che a queste congruenze quadratiche, i numeri ξ debbono anche soddisfare ad una congruenza lineare, che ritroviamo colla considerazione seguente: Fra i numeri interi di $k(\theta)$ vi è anche il numero 1, ed esistono quindi n interi razionali $h_1, h_2, \ldots, h_n$, perfettamente determinati e *primi necessariamente fra loro*, tali che si abbia

$$h_1 \omega_1 + h_2 \omega_2 + \ldots + h_n \omega_n = 1 . \tag{1}$$

Questa, per i numeri ξ, si cambia nella congruenza lineare in questione

$$h_1 \xi_1 + h_2 \xi_2 + \ldots + h_n \xi_n \equiv 1 \pmod{m} . \tag{II*}$$

Così adunque, affinchè esista un ideale primario assoluto A di norma $NA = m$ *è necessario che esistano n numeri razionali interi* $\xi_1, \xi_2, \ldots, \xi_n$ *che soddisfino, rispetto al modulo* m, *alle* $\frac{n(n+1)}{2}$ *congruenze quadratiche* (II), *ed alla congruenza lineare* (II*).

Ed ora passiamo a dimostrare che tali condizioni, riconosciute come necessarie, sono anche sufficienti.

5. — Supponiamo che i numeri razionali interi $\xi_1, \xi_2 \ldots \xi_n$ soddisfino le congruenze (II) e (II*), e disponiamo dei multipli interi arbitrarii di m, che possono aggiungersi alle ξ_i, in modo da convertire la congruenza (II*) nella eguaglianza

$$h_1 \xi_1 + h_2 \xi_2 + \ldots + h_n \xi_n = 1 - m , \tag{2}$$

il che è sempre possibile perchè $h_1, h_2 \ldots h_n$ sono primi fra loro (1).

Consideriamo allora il *modulo*

$$A = [\xi_1 - \omega_1, \xi_2 - \omega_2, \ldots, \xi_n - \omega_n]$$

e dimostriamo che esso è un ideale primario assoluto di norma $NA = m$.

In primo luogo si osservi che dalle (1) e (2), sottratte, risulta

$$h_1 (\xi_1 - \omega_1) + h_2 (\xi_2 - \omega_2) + \ldots + h_n (\xi_n - \omega_n) = - m , \tag{3}$$

e per ciò intanto il numero m appartiene al modulo A.

Che poi A sia un ideale, lo proviamo dimostrando che ogni prodotto

$$\omega_k (\xi_i - \omega_i)$$

appartiene al modulo stesso. Difatti

$$\omega_k (\xi_i - \omega_i) = \xi_i (\omega_k - \xi_k) - \sum_l c_{ik}^{(l)} \omega_k + \xi_i \xi_k ,$$

e, per la (II),

$$\xi_i \xi_k = \sum_l c_{ik}^{(l)} \xi_l + qm \ (q \text{ intero}) .$$

(1) Se $\xi'_1, \xi'_2, \ldots, \xi'_n$ soddisfano alle (II), (II*), sarà

$$h_1 \xi'_1 + h_2 \xi'_2 + \ldots + h_n \xi'_n = 1 + q\, m \ (q \text{ intero}).$$

Presi allora gli interi $c_1, c_2 \ldots c_n$ in modo che sia

$$h_1 c_1 + h_2 c_2 + \ldots + h_n c_n = 1 - q ,$$

pongasi $\xi_i = \xi'_i - c_i m$ e ne risulterà la (2).

Si ha dunque, per la precedente e per la (3),

$$\omega_k(\xi_i - \omega_i) = \xi_i(\omega_k - \xi_k) + \sum_l c_{ik}^{(l)}(\xi_l - \omega_l) - q\sum_i h_i(\xi_i - \omega_i),$$

e questo è un numero in A. Dunque A è un *ideale*. Esso è poi primario assoluto perchè

$$\omega_i \equiv \xi_i \,(\text{mod. A}),$$

e quindi un numero intero qualunque di $k(\theta)$

$$\omega = c_1\omega_1 + c_2\omega_2 + \ldots + c_n\omega_n$$

è congruo (mod. A) col numero razionale

$$c_1\xi_1 + c_2\xi_2 + \ldots + c_n\xi_n$$

Resta da ultimo da provare che $NA = m$, e per questo si osservi che la base di A è data dagli n numeri

$$\alpha_i = \xi_i - \omega_i = \xi_i(h_1\omega_1 + h_2\omega_2 + \ldots + h_n\omega_n) - \omega_i;$$

e quindi, nella sostituzione aritmetica che li lega alla base del corpo

$$\alpha_i = \sum_k c_{ik}\omega_k,$$

si ha

$$c_{ik} = h_k\xi_i - \varepsilon_{ik} \quad (\varepsilon_{ii} = 1,\ \varepsilon_{ik} = 0 \text{ per } i \neq k).$$

Il modulo C di questa sostituzione è

$$C = \begin{vmatrix} h_1\xi_1 - 1 & h_2\xi_1 & \ldots & h_n\xi_1 \\ h_1\xi_2 & h_2\xi_2 - 1 & \ldots & h_n\xi_2 \\ \ldots & \ldots & \ldots & \ldots \\ h_1\xi_n & h_2\xi_n & \ldots & h_n\xi_n - 1 \end{vmatrix}$$

ed ha per valore

$$C = (-1)^n\{1 - \sum h_i\xi_i\} = (-1)^n m.$$

Il suo valore assoluto è m, e dà appunto la norma dell'ideale.

I risultati stabiliti in questi due ultimi numeri comprendono quelli ottenuti al principio della Nota citata. In questa (n°. 5 e seg^ti. *Journal de mathématiques*) ho inoltre dimostrato che la risoluzione del sistema di congruenze (II) e (II*) si riduce essenzialmenle a quella di un'unica congruenza

$$f(\xi) \equiv 0 \,(\text{mod. } m)$$

di grado eguale al grado n del corpo.

Questa, se θ è il numero generatore del campo, radice dell'equazione irriducibile $f(x) = 0$, si ottiene mutando quest'equazione in congruenza (mod. m). Qui per altro è essenziale la condizione che la norma m dell'ideale da costruirsi sia un numero primo coll'*indice* del numero generatore θ (vedi loc. cit.).