JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

LUIGI BIANCHI

Sugli ideali primarii assoluti in un corpo algebrico

Journal de mathématiques pures et appliquées 9^e série, tome 1 (1922), p. 1-18.
<http://www.numdam.org/item?id=JMPA_1922_9_1__1_0>

JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES.

Sugli ideali primarii assoluti in un corpo algebrico;

PER LUIGI BIANCHI.
(Pisa.)

1. Sia definito un corpo algebrico $k(\theta)$ di grado n, mediante un suo numero intero generatore θ, radice di un' equazione irriducibile

$$(A) \qquad f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0,$$

con primo coefficiente $a_0 = 1$, e gli altri razionali interi.

Un qualunque ideale A del corpo contiene infiniti numeri razionali (interi), tutti multipli del più piccolo di essi, e fra questi numeri vi è sempre la *norma* NA dell' ideale. Diremo che l'ideale A è *primario assoluto* (1), quando NA coïncide col più piccolo numero razionale

(1) In generale si dice primario un ideale quando nessun numero naturale > 1 divide tutti i suoi numeri. Se NA è il più piccolo razionale in A, l'ideale è certamente primario; ma non sussiste la proprietà inversa, salvo nel caso dei corpi quadratici, ove *qualunque ideale primario è anche assoluto*.

in A. Osserviamo subito che, fra gli ideali primarii assoluti, si trovano tutti gli ideali primi P di *primo grado*, perchè allora $NP = p$ dove p è il numero primo naturale coordinato a P, ed è al tempo stesso il più piccolo numero razionale in P. Si vedrà poi (n° 5) che ogni ideale primario assoluto, decomposto in ideali primi, dà luogo a soli ideali primi di primo grado.

In questa nota vogliamo ricercare gli ideali primarii assoluti A di $k(0)$, la cui norma eguaglia un intero positivo fissato m

$$NA = m.$$

Per questa, come per tutte le ricerche che concernono la costruzione di ideali in $k(0)$, è essenziale ricorrere alle *costanti* di *composizione* di una base intera *minima* del corpo

$$[\omega_1, \omega_2, \ldots, \omega_n], \tag{1}$$

sicchè ogni altro intero ω di $k(0)$ si ottiene, in modo univoco, dalla formola

$$\omega = h_1\omega_1 + h_2\omega_2 + \ldots + h_n\omega_n, \tag{2}$$

dove i coefficienti h_i sono razionali interi. In particolare si pongono sotto la forma (2) gli $\frac{n(n+1)}{2}$ prodotti $\omega_i\omega_k$ di due elementi qualunque (diversi od eguali) della base (1), e noi scriveremo le corrispondenti formole così

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

Questi $\frac{n^2(n+1)}{2}$ numeri *razionali interi* $\gamma_{ik}^{(l)}$ si diranno appunto le costanti di composizione della base (1)(1).

In generale, assegnata la base (1), per trovare un *qualunque*

(1) Osservo qui incidentalmente che le costanti $\gamma_{ik}^{(l)}$ si possono opportunamente indicare coi *simboli a tre indici* $\left\{ \begin{matrix} ik \\ l \end{matrix} \right\}$ di Christoffel nella teoria delle forme differenziali quadratiche, per la ragione seguente. Esiste, nello spazio *Euclideo* S_n a n dimensioni, un conveniente sistema di coordinate curvilinee

ideale A di norma data

$$NA = m,$$

se ne cercherà una base

$$[\alpha_1, \alpha_2, \ldots, \alpha_n],$$

che si potrà esprimere sotto la forma *ridotta*

$$(3)\qquad \begin{cases} \alpha_1 = a_1\ \omega_1, \\ \alpha_2 = a_{21}\omega_1 + a_2\ \omega_2, \\ \alpha_3 = a_{31}\omega_1 + a_{32}\omega_2 + a_3\omega_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_n = a_{n1}\omega_1 + a_{n2}\omega_2 + \ldots + a_{n,n-1}\omega_{n-1} + a_n\omega_n. \end{cases}$$

I coefficienti a_i, a_{ik} della sostituzione lineare a destra sono tutti interi razionali; quelli $a_1, a_2, \ldots, a_n$ della diagonale principale *positivi*, con prodotto eguale alla norma assegnata

$$(4)\qquad a_1 a_2 \ldots a_n = m,$$

mentre i secondarii in ciascuna colonna nella i^{ma} per esempio

$$(5)\qquad a_{i+1,i},\quad a_{i+2,i},\quad \ldots\ldots\quad a_{n,i}\qquad (i = 1, 2, \ldots, n-1),$$

$(u_1, u_2, \ldots, u_n)$, per le quali il ds^2 dello spazio S_n

$$ds^2 = \Sigma\, b_{ik}(u)\, du_i\, du_k$$

ha una tale forma che i simboli a tre indici $\left\{ \begin{matrix} ik \\ l \end{matrix} \right\}$ risultano *costanti*, precisamente $= \gamma_{ik}^{(l)}$. Se con $x_1, x_2, \ldots, x_n$ indichiamo coordinate Cartesiane in S_n, ciascuna di queste soddisfa al sistema, completamente integrabile, di equazioni alle derivate parziali

$$\frac{\partial^2 x}{\partial u_i\, \partial u_k} = \sum_l \left\{ \begin{matrix} ik \\ l \end{matrix} \right\} \frac{\partial x}{\partial u_i}\, \frac{\partial x}{\partial u_k}.$$

Oltre la $x = \text{cost.}$ se ne hanno subito le altre n soluzioni indipendenti

$$x_r = e^{\omega_1^{(r)} u_1 + \omega_2^{(r)} u_2 + \ldots + \omega_n^{(r)} u_n}\qquad (r = 1, 2, \ldots, n)$$

dove $[\omega_1^{(r)}, \omega_2^{(r)}, \ldots, \omega_n^{(r)}]$ sono le n basi degli n corpi coniugati. Pel Jacobiano $I(x_1, x_2, \ldots, x_n)$ si ha subito

$$I(x_1, x_2, \ldots, x_n) = x_1 x_2 \ldots x_n \sqrt{(D)},$$

dove D è il numero fondamentale del corpo, e questo Jacobiano è in effetto $\neq 0$.

possono surrogarsi ciascuno con un qualunque numero congruo $(\mathrm{mod}\, a_i)$. Se questi coefficienti soddisferanno alle condizioni perché $[\alpha_1, \alpha_2, \ldots, \alpha_n]$ sia l'effettiva base di un ideale, questo sarà perfettamente determinato dai valori scelti per $a_1, a_2, \ldots, a_n$, e dai minimi resti positivi $(\mathrm{mod}\, a_i)$ dei numeri (5).

La base (1) del corpo può variarsi in infiniti modi, assoggettandola ad una arbitraria sostituzione *aritmetica* unimodulare. Per lo scopo nostro conviene sceglierla (come sempre è possibile) in guisa che fra in numeri della base (1) figuri il n° 1, e sia per esempio $\omega_1 = 1$. In tal caso, nelle formole (I) quelle costanti di composizione $\gamma_{ik}^{(l)}$ che hanno $k = 1$ $(0, i = 1)$ presentano i valori

$$(6) \qquad \begin{cases} \gamma_{i1}^{(l)} = 0 & \text{per} \quad i \neq l, \\ \gamma_{i1}^{(l)} = 1 & \text{per} \quad i = l. \end{cases}$$

Con questa scelta $[1, \omega_2, \omega_3, \ldots, \omega_n]$ della base, nello schema dei coefficienti della (3)

$$(7) \qquad \begin{vmatrix} a_1 & 0 & 0 & \ldots & 0 \\ a_{21} & a_2 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & \ldots & a_n \end{vmatrix}$$

il primo elemento a_1 in diagonale dà il minimo numero razionale contenuto nell' ideale e gli altri $a_2, a_3, \ldots, a_n$ sono tutti divisori di a_1.

2. Scelta la base in quest' ultimo modo più semplice $(\omega_1 = 1)$, vogliasi costruire un ideale primario assoluto A, con $\mathrm{NA} = m$. Per quanto ora si è detto, dovremo avere nello schema (7) $a_1 = m$, indi per la (4)

$$a_2 = a_3 = \ldots = a_n = 1,$$

e tutti gli elementi secondarii nella 2^a, 3^a, ..., $(n-1)^{ma}$ colonna, ridotti mod 1, potranno rendersi $= 0$. Scriveremo lo schema sotto la forma

$$\begin{vmatrix} m & 0 & 0 & \ldots & 0 \\ -\xi_2 & 1 & 0 & \ldots & 0 \\ -\xi_3 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -\xi_n & 0 & 0 & \ldots & 1 \end{vmatrix},$$

dove $\xi_2, \xi_3, \ldots, \xi_n$ saranno numeri razionali interi presi (mod m). La base dell' ideale A avrà pertanto la forma

$$A = [m, \omega_2 - \xi_2, \omega_3 - \xi_3, \ldots, \omega_n - \xi_n], \tag{8}$$

e saranno ora da ricercare le condizioni necessarie e sufficienti, a cui debbono soddisfare gli $n - 1$ numeri incogniti

$$\xi_2, \quad \xi_3, \quad \ldots, \quad \xi_n,$$

affinchè il *modulo* (8) sia un effettivo ideale. Per questo occorre e basta che ciascuno degli n elementi della base (8), moltiplicato per un qualunque ω_h, dia un numero del modulo (8), cioè si ponga sotto la forma

$$m x_1 + \sum_{l=2}^{l=n} (\omega_l - \xi_l) x_l,$$

essendo $x_1, x_2, \ldots, x_n$ convenienti numeri razionali interi, che scriviamo anche

$$m x_1 - \sum_{l=2}^{l=n} \xi_l x_l + \sum_{l=2}^{l=n} x_l \omega_l. \tag{9}$$

Pel moltiplicatore $\omega_1 = 1$ questo non implica condizione alcuna, e medesimamente pei prodotti

$$m \omega_k = m \xi_k + m(\omega_k - \xi_k),$$

onde bastera esprimere che ogni prodotto

$$(\omega_i - \xi_i)\omega_k \quad \text{per} \quad i, k = 2, 3, \ldots, n$$

deve porsi sotto la forma (9).

Ma, per le formole (I) di composizione, abbiamo

$$(\omega_i - \xi_i)\omega_k = \sum_{l=1}^{l=n} \gamma_{ik}^{(l)} \omega_l - \xi_i \omega_k,$$

e nel confronto colla espressione (9), essendo $\omega_1 = 1, \omega_2, \ldots, \omega_n$ indipendenti, dobbiamo eguagliare i coefficienti corrispondenti di cia-

scuna ω_l dalle due parti ($l = 1, 2, \ldots, n$); questo ci dà le relazioni

$$m x_1 = \sum_{l=2}^{l=n} \xi_l x_l + \gamma_{1k}^{(1)},$$

$$\begin{aligned} x_l &= \gamma_{1k}^{(l)} \quad \text{per} \quad l \neq k \\ x_k &= \gamma_{1k}^{(k)} - \xi_l \quad (l = k) \end{aligned} \qquad (l \geq 2).$$

Se nella prima di queste sostituiamo per $x_2, x_3, \ldots, x_n$ i valori dati dalle ultime, rimangono, quali condizioni per le incognite $\xi_2, \xi_3, \ldots, \xi_n$, le seguenti congruenze quadratiche rispetto al modulo m

$$\xi_i \xi_k \equiv \gamma_{ik}^{(1)} + \sum_{l=2}^{l=n} \gamma_{ik}^{(l)} \xi_k \pmod{m} \tag{10}$$

$$(i, k = 2, 3, \ldots, n).$$

3. Da questa semplice analisi è già lecito intanto concludere :

Affinchè esistano ideali primarii assoluti A *con* $\mathrm{NA} = m$, *è necessario e sufficiente che, nelle* $n-1$ *incognite*

$$\xi_2, \quad \xi_3, \quad \ldots, \quad \xi_n,$$

ammetta soluzioni il sistema delle $\frac{(n-1)n}{2}$ *congruenze quadratiche* (10). *Esisteranno tanti di questi ideali* A *quante soluzioni incongrue avrà il sistema* (10), *e per ogni soluzione si avrà dalla* (8) *il corrispondente ideale* A *espresso per la sua base.*

Di qui, senza ancora entrare nella discussione del sistema (10) vedi numeri segmenti), possiamo subito dedurre alcune conseguenze notevoli.

Sia A un ideale primario assoluto con $\mathrm{NA} = m$, e siano $\xi_2, \xi_3, \ldots, \xi_n$ i corrispondenti valori delle ξ, che soddisferanno alle (10). Prendiamo un qualunque divisore *puro* m_1 di m, sia $1 < m_1 < m$. I medesimi valori per $\xi_2, \xi_3, \ldots, \xi_n$ soddisferanno, *a fortiori*, le (10) scritte rispetto al modulo m_1, e quindi sarà

$$\mathrm{A}_1 = [m_1, \omega_2 - \xi_2, \omega_3 - \xi_3, \ldots, \omega_n - \xi_n]$$

un altro ideale primario assoluto, che avrà

$$NA_1 = m_1.$$

I numeri della base (8) di A sono tutti contenuti in A_1, gli ultimi $n-1$ come comuni, il primo m come multiplo di m_1; dunque A è contenuto in A_1, ossia divisibile per A_1. Ma ora se

$$m = m_1 m_2,$$

per la ragione stessa anche l'ideale

$$A_2 = [m_2, \omega_2 - \xi_2, \ldots, \omega_n - \xi_n]$$

è primario assoluto ed è divisore di A. Precisamente dimostriamo che si ha

$$A = A_1 A_2,$$

osservando in primo luogo che i due ideali a sinistra e a destra hanno egual norma

$$NA = m, \qquad N(A_1 A_2) = NA_1 \, NA_2 = m_1 m_2.$$

In secondo luogo poi il prodotto $A_1 A_2$ è generato dagli n^2 numeri

$$m_1 m_2 = m, \qquad m_1(\omega_i - \xi_i), \qquad m_2(\omega_i - \xi_i), \qquad (\omega_i - \xi_i)(\omega_k - \xi_k),$$

che sono tutti contenuti in A, ed è per ciò $A_1 A_2$ divisibile per A; ma, avendo la stessa norma, coincide con A.

Applicando ripetutamente questo risultato, si vede che in generale:

Se la norma m dell' ideale primario assoluto

$$A = [m, \omega_2 - \xi_2, \ldots, \omega_n - \xi_n)$$

si scinde, in un qualunque modo, nel prodotto di r fattori

$$m = m_1 m_2 \ldots m_r,$$

corrispondentemente l'ideale A *si può scindere nel prodotto degli r ideali primarii assoluti* $A_1, A_2, \ldots, A_r$, *di rispettive norme* $m_1, m_2, \ldots, m_r$

$$A = A_1 A_2 \ldots A_r,$$

dove

$$A_i = [m_i, \omega_2 - \xi_2, \ldots, \omega_n - \xi_n].$$

In particolare, se si scinde m nei suoi fattori primi diversi p_1, p_2, ..., p_s, colla formola

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

si ha immediatamente l'ideale A decomposto in ideali primi di *primo grado*

$$P_i = [p_i, \omega_2 - \xi_2, \dots, \omega_n - \xi_n] \qquad (i = 1, 2, \dots, s)$$

colla formola corrispondente

$$A = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_s^{\alpha_s}.$$

Così è confermata l'asserzione al n° **1**.

4. I risultati ora ottenuti, rispetto alla decomposizione di un ideale primario assoluto nel prodotto di altri della stessa specie, possono in certo modo invertirsi, sotto la condizione che appare dall' enunciato seguente :

Se più ideali primarii assoluti hanno le norme prime fra loro due a due, anche il loro prodotto è un ideale primario assoluto.

Basterà dimostrare la proprietà per due tali ideali

$$A_1 = [m_1, \omega_2 - \xi_2^{(1)}, \omega_3 - \xi_3^{(1)}, \dots, \omega_n - \xi_n^{(1)}],$$
$$A_2 = [m_2, \omega_2 - \xi_2^{(2)}, \omega_3 - \xi_3^{(2)}, \dots, \omega_n - \xi_n^{(2)}],$$

le cui norme m_1, m_2 si suppongano prime fra loro. Qui $(\xi_2^{(1)}, \xi_3^{(1)}, \dots, \xi_n^{(1)})$ indica una soluzione delle congruenze (10), scritte *rispetto al modulo* m_1, e similmente $(\xi_2^{(2)}, \dots, \xi_n^{(2)})$ una soluzione delle medesime congruenze (10) rispetto al modulo m_2. Ma allora, essendo m_1, m_2 primi fra loro, possiamo determinare $n-1$ altri numeri $\xi_2, \xi_3, \dots, \xi_n$ che soddisfino alle congruenze simultanee

$$\xi_i \equiv \xi_i^{(1)} \pmod{m_1}, \qquad \xi_i \equiv \xi_i^{(2)} \pmod{m_2}$$
$$(i = 2, 3, \dots, n);$$

e allora questi numeri soddisferanno alle medesime congruenze (10) rispetto a ciascuno dei moduli m_1, m_2 e per ciò anche rispetto al loro minimo multiplo comune $m = m_1 m_2$. Per quanto si è visto sopra, il prodotto $A_1 A_2$ è l'ideale primario assoluto

$$A = [m, \omega_2 - \xi_2, \dots, \omega_n - \xi_n]. \qquad \text{C. D. D.}$$

Del resto la proprietà ora segnalata discende da questa più generale :

Se A_1, A_2 *sono due ideali qualunque, contenenti rispettivamente come minimi numeri razionali i numeri* m_1, m_2, primi fra loro, *nell' ideale prodotto* $A_1 A_2$ *il minimo numero razionale contenuto è il prodotto* $m_1 m_2$.

Intanto $m_1 m_2$ è certamente contenuto in $A_1 A_2$; d'altra parte, il minimo numero razionale m contenuto in A è contenuto tanto in A_1 che in A_2, indi multiplo di m_1 e di m_2, per ciò anche del loro prodotto.

5. Si è visto che l'esistenza di ideali primarii assoluti nel corpo $k(0)$, con norma assegnata $= m$, è subordinata alla risolubilità del sistema di congruenze (10) $(\mathrm{mod}\, m)$ nelle $n-1$ incognite $\xi_2, \xi_3, \ldots, \xi_n$. Si vedrà ora che, sotto una condizione la quale verrà subito specificata, il sistema (10) può sostituirsi con una sola congruenza di grado n in una sola incognita ξ, e questa è semplicemente la $f(\xi) \equiv 0 (\mathrm{mod}\, m)$, che risulta dall' equazione fondamentale (A) cangiandola in congruenza $(\mathrm{mod}\, m)$.

Prima però ci conviene scrivere le (10) sotto una forma più simmetrica, che viene suggerita del confronto colle formole (I) di composizione. Oltre ai numeri $\xi_2, \xi_3, \ldots, \xi_n$ s'introduca un n^{mo} numero ξ_1, e in corrispondenza ad $\omega_1 \equiv 1$, facciamo

$$\xi_1 \equiv 1 \qquad (\mathrm{mod}\, m).$$

Così le (10) potranno scriversi per tutti i valori $1, 2, \ldots, n$ degli indici i, k sotto la forma

$$(\mathrm{I}^*) \qquad \xi_i \xi_k \equiv \sum_{\rho=1}^{l=n} \gamma_{ik}^{(l)} \xi_l \qquad (\mathrm{mod}\, m)$$
$$(i, k = 1, 2, \ldots, n),$$

e queste risultano dalle (I) riducendole a congruenze $(\mathrm{mod}\, m)$, col sostituire agli interi algebrici ω_i i numeri interi razionali ξ_i.

Siccome $\xi_1 \equiv 1 (\mathrm{mod}\, m)$, le congruenze ($\mathrm{I}^*$) aggiunte alle (10) (quelle con $i \circ k = 1$) sono identità, a causa delle formole (6).

Si osservi ancora che pure avendo fatto uso, nella deduzione delle (I*) dalle (I), della base speciale con $\omega_1 = 1$, la relazione indicata vale comunque cangiando la base $[\omega_1, \omega_2, \ldots, \omega_n]$ con una sostituzione aritmetica unimodulare, quando la stessa sostituzione si operi sopra $\xi_1, \xi_2, \ldots, \xi_n$.

Per una qualunque base $[\omega_1, \omega_2, \ldots, \omega_n]$, affinchè esistano ideali primarii assoluti di norma $= m$, è necessario che il sistema di congruenze quadratiche (I*) ammetta soluzioni $(\xi_1, \xi_2, \ldots, \xi_n)$ non tutte nulle (mod m).

Ed ora, per ridurre il sistema (I*) ad una sola congruenza, ricorreremo alla nozione di *indice* C del numero generatore θ (Dedekind). Questo indice C è il numero razionale intero

$$C = \sqrt{\frac{d(\theta)}{D}},$$

dove $d(\theta)$ indica il discriminante del numero θ e D il numero fondamentale del corpo.

Ciò premesso, noi faremo l'ipotesi che:

La norma m dell' ideale primario assoluto A *da costruirsi sia un numero primo coll' indice* C *di* θ.

Il numero stesso C si presenta anche, sotto altra forma, come modulo della sostituzione lineare che esprime i numeri

$$1, \quad \theta, \quad \theta^2, \quad \ldots, \quad \theta^{n-1},$$

formanti la base dell' *ordine o anello* di numeri $R(\theta)$ per la base $[\omega_1, \omega_2, \ldots, \omega_n]$. Scriviamo questa sostituzione

$$(11) \qquad \begin{cases} 1 = c_{11}\omega_1 + c_{12}\omega_2 + \ldots + c_{1n}\omega_n, \\ \theta = c_{21}\omega_1 + c_{22}\omega_2 + \ldots + c_{2n}\omega_n, \\ \theta^2 = c_{31}\omega_1 + c_{32}\omega_2 + \ldots + c_{3n}\omega_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \theta^{n-1} = c_{n,1}\omega_1 + c_{n,2}\omega_2 + \ldots + c_{n,n}\omega_n, \end{cases}$$

dove i coefficienti c_{ik} sono razionali interi.

Il determinante $|C_{ik}|$, che è diverso da zero per l'irriducibilità

della (A), si può supporre positivo (1), ed eguaglia appunto l'indice C del numero 0

$$C = |c_{lk}|.$$

6. Per semplificare le deduzioni seguenti, supponiamo, come al n° **1**, che la base sia scelta con $\omega_1 = 1$, onde intanto pei coefficienti della prima orizzontale nelle (11) avremo

$$c_{11} = 1, \qquad c_{12} = c_{13} = \ldots = c_{1n} = 0. \tag{12}$$

Osserviamo che, conosciuti i coefficienti

$$c_{21}, \quad c_{22}, \quad \ldots, \quad c_{2n}$$

della seconda orizzontale, quelli delle rimanenti si esprimeranno per questi e per le costanti di composizione $\gamma_{ik}^{(l)}$ in modo perfettamente determinato. Così per quelli della terza orizzontale, avendosi

$$\theta^2 = \sum_i c_{2i}\omega_i \sum_k c_{2k}\omega_k = \sum_{i,k,l} \gamma_{ik}^{(l)}\, c_{2i}\, c_{2k}\, \omega_l,$$

risulta

$$c_{3l} = \sum_{i,k} \gamma_{ik}^{(l)}\, c_{2i}\, c_{2k};$$

similmente

$$c_{3l} = \sum_{i,k} \gamma_{ik}^{(l)}\, c_{3i}\, c_{2k}, \ldots.$$

Conviene poi osservare che al quadro (11) possiamo aggiungere una $(n+1)^{ma}$ orizzontale

$$\theta^n = c_{n+1,1}\omega_1 + c_{n+1,2}\omega_2 + \ldots + c_{n+1,n}\omega_n,$$

ed a causa della identità $f(\theta) = 0$, avremo

$$c_{n+1,i} + a_1 c_{n,i} + a_2 c_{n-1,i} + \ldots + a_n c_{1,i} = 0 \qquad (i = 1, 2, \ldots, n). \tag{13}$$

Ora al posto delle $n-1$ incognite $\xi_2, \xi_3, \ldots, \xi_n$, coll'aggiunta al solito di $\xi_1 \equiv 1 \pmod m$, introduciamo la nuova incognita

$$\xi \equiv c_{21}\xi_1 + c_{22}\xi_2 + \ldots + c_{2n}\xi_n \pmod m,$$

(1) Basta, in caso contrario, cangiare di segno una delle ω_i.

e di questa formiamo le successive potenze, tenendo conto delle formole (I*) e delle osservazioni precedenti. Ne dedurremo le congruenze corrispondenti alle formole (11) :

$$(11^*)\qquad \begin{cases} 1 \equiv c_{11}\xi_1 + c_{12}\xi_2 + \ldots + c_{1n}\xi_n \\ \xi \equiv c_{21}\xi_1 + c_{22}\xi_2 + \ldots + c_{2n}\zeta_n \\ \xi^2 \equiv c_{31}\xi_1 + c_{32}\xi_2 + \ldots + c_{3n}\xi_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \xi^{n-1} \equiv c_{n1}\xi_1 + c_{n2}\xi_2 + \ldots + c_{nn}\xi_n \end{cases} \pmod m,$$

le quali si ottengono dalle (11) come le (I*) dalle (I) e cioè convertendole in congruenze (mod m) col sostituire alle ω_i le ξ_i (1).

Costruendo ancora ξ^n, avremo

$$\xi^n \equiv c_{n+1,1}\xi_1 + c_{n+1,2}\xi_2 + \ldots + c_{n+1,n}\xi_n \pmod m,$$

dopo di che dalle identità (13) risulta :

L'incognita ξ *deve essere radice della congruenza*

$$(A^*)\quad f(\xi) = \xi^n + a_1\xi^{n-1} + a_2\xi^{n-2} + \ldots + a_{n-1}\xi + a_n \equiv 0 \pmod m,$$

che si forma dall' equazione fondamentale (A) *cangiando questa in congruenza* (mod m).

Non puó dunque esistere alcun ideale primario assoluto di norma $= m$, se non ha radici la congruenza (A*); e questo vale anche se m non è primo con C, poichè dell' ulteriore ipotesi non si è fin qui fatto uso. Ma supponendola ora soddisfatta, mostriamo come si inverte il risultato precedente, e la condizione trovata necessaria risulta anche sufficiente.

7. Risolvendo il sistema delle n equazioni lineari (11), rispetto ad $\omega_1, \omega_2, \ldots, \omega_n$, otteniamo

$$(B)\qquad C\omega_k = C_{1k} + C_{2k}\theta + \ldots + C_{n,k}\theta^{n-1} \qquad (k = 1, 2, \ldots, n),$$

avendo indicato con C_{ik} il complemento algebrico dell' elemento c_{ik} nel determinante C.

---

(1) La prima delle (11*) è identica, a causa delle (12) e di $\xi_1 \equiv 1 \pmod m$.

E similmente dalle corrispondenti congruenze (11*) avremo risolvendo

$$(B^*) \quad C\xi_k \equiv C_{1k} + C_{2k}\xi + \ldots + C_{n,k}\xi^{n-1} \pmod{m} \qquad (k = 1, 2, \ldots, n).$$

Siccome C *è primo col modulo* m, queste fissano i valori di $\xi_1, \xi_2, \ldots, \xi_n$ appena fissato quello di ξ. Di più, in riguardo alla ξ_1, siccome dalle (12) [ô anche dalle (B)] segue

$$C_{11} = C, \qquad C_{21} = C_{31} = \ldots = C_{n1} = 0,$$

e la (B*) per $k = 1$ dà

$$C(\xi_1 - 1) \equiv 0 \pmod{m},$$

da cui $\xi_1 \equiv 1 \pmod{m}$.

Ora è facile dimostrare che, se ξ è una radice della congruenza

$$f(\xi) \equiv 0 \pmod{m},$$

le ξ_k, cosi calcolate univocamente dalle (B*), verranno a soddisfare alle congruenze quadratiche (I*).

Difatti, siccome le formole di composizione (I) sono conseguenze delle (B) e dell' essere θ radice di $f(\theta) = 0$, cosi pure dalle (B*) e dal fatto che ξ soddisfa alla $f(\xi) \equiv 0 \pmod{m}$ discendono ora le congruenze quadratiche (I*).

Abbiamo dunque :

Se il numero m *è primo coll' indice* C *del numero* θ, *esistono nel corpo* $k(\theta)$ *tanti ideali primarii assoluti colla norma* $= m$, *quante radici diverse* (*incongrue*) *possiede la congruenza*

$$f(\xi) \equiv 0 \pmod{m};$$

e per ciascuna tale radice ξ, *si ha l'ideale* A *corrispondente espresso per la sua base colla formola*

$$(14) \qquad A = [m, \omega_2 - \xi_2, \ldots, \omega_n - \xi_n],$$

dove i numeri $\xi_2, \xi_3, \ldots, \xi_n$ *si calcolano univocamente* (mod m) *dalle congruenze* (B*).

Si può anche individuare l'ideale A, invece che per la base, per due

suoi numeri di cui sia il massimo comun divisore. Dalle formole

$$\begin{aligned} \theta &= c_{21} + c_{22}\omega_2 + \ldots + c_{2n}\omega_n \\ \xi &\equiv c_{21} + c_{22}\xi_2 + \ldots + c_{2n}\xi_n \end{aligned} \pmod{m},$$

sottraendo risulta

$$\theta - \xi = qm + c_{22}(\omega_2 - \xi_2) + \ldots + c_{2n}(\omega_n - \xi_n)$$

con q intero razionale, e per la (14) questo è un numero dell'ideale A. Ora dimostriamo:

L'ideale A *è il massimo comun divisore dei due numeri* m, $\theta - \xi$, *o esprimendo in simboli*,

$$A = (m, \theta - \xi).$$

Per questo dovremo provare che i due ideali A e $(m, \theta - \xi)$ si contengono l'un l'altro. Che il secondo sia contenuto nel primo è evidente, perchè vi sono contenuti i due numeri generatori m, $\theta - \xi$. In secondo luogo dalle (B), (B*), sottraendo, abbiamo

$$C(\omega_k - \xi_k) = qm + \left[C_{2k} + C_{3k}\frac{\theta^2 - \xi^2}{\theta - \xi} + \ldots + C_{n,k}\frac{\theta^{n-1} - \xi^{n-1}}{\theta - \xi}\right](\theta - \xi),$$

dove q è un numero razionale intero, e a destra il moltiplicatore di $\theta - \xi$ è un intero μ di $k(\theta)$, onde dalla formola

$$C(\omega_k - \xi_k) = qm + \mu(\theta - \xi)$$

risulta che $C(\omega_k - \xi_k)$ è un numero dell' ideale $(m, \theta - \xi)$. Siccome poi C è primo con m, possiamo prendere due interi razionali t, u tali che sia

$$Ct = 1 + mu,$$

e nell' ideale $(m, \theta - \xi)$ sarà pure contenuto il numero

$$Ct(\omega_k - \xi_k) = \omega_k - \xi_k + u(\omega_k - \xi_k)m,$$

quindi anche

$$\omega_k - \xi_k = Ct(\omega_k - \xi_k) - u(\omega_k - \xi_k)m$$

come differenza di due numeri dell' ideale.

Dunque tutti gli n numeri della base (14) di A si trovano nell' ideale $(m, \theta - \xi)$ ed A stesso è contenuto in $(m, \theta - \xi)$, e si conclude

appunto

$$A = (m, \theta - \xi).$$

8. Secondo i risultati al n° **3**, gli elementi coi quali si compongono gli ideali primarii assoluti sono esclusivamente gli ideali primi di primo grado. Si sa che :

In ogni corpo algebrico esistono infiniti ideali primi di primo grado.

La proposizione si stabilisce in generale col sussidio dell'aritmetica analitica (¹). Qui vogliano dimostrarla, almeno in un caso particolare ma assai esteso, come si vedrà, con mezzi puramente aritmetici. Il caso che vogliamo trattare è il seguente : *supponiamo che a numero generatore del corpo* $k(\theta)$ possa *scegliersi un' unità.* Tale circostanza si verifica sempre, in particolare, quando fra gli n corpi coniugati

$$k^{(1)}, \quad k^{(2)}, \quad \ldots, \quad k^{(n)}$$

uno almeno è reale. Questo deriva dal teorema fondamentale di Dirichlet per l'esistenza delle unità, come segue. Attribuiamo il corpo reale k al primo gruppo A del teorema di Dirichlet, e tutti i rimanenti al secondo gruppo B. Esiste in $k(\theta)$, pel teorema ricordato, un' unità ε il cui modulo è > 1, mentre tutti i moduli dei coniugati (appartenenti al gruppo B) sono invece < 1. In queste condizioni, il numero ε non può eguagliare alcuno dei suoi coniugati, ed è quindi di grado n (primitivo), ossia un numero generatore del corpo come si voleva.

Scelto dunque a numero generatore θ del corpo un' unità, avendosi $N\theta = \pm 1$, il valore assoluto dell' ultimo coefficiente a_n, nell' equazione fondamentale (A), sarà $= 1$, scriviamo

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x \pm 1. \tag{15}$$

Ora dimostriamo :

Scelto un qualunque numero razionale intero (positivo) μ, *si può trovare un numero primo* p, *che non divida* μ, *e pel quale la congruenza* $f(\xi) \equiv 0 \pmod{p}$ *sia solubile.*

(¹) Vi WEBER, *Lehrbuch der Algebra*, II^e Auflage, II^{er} Bd. § 197, S^e 727.

Pongasi nella (15) per x un intero arbitrario multiplo di μ.

$$x = q\mu \qquad (q \text{ intero arbitrario}).$$

Il numero intero che ne risulta

$$(16) \qquad N = f(q\mu) = q^n\mu^n + a_1 q^{n-1}\mu^{n-1} + \ldots + a_{n-1} q\mu \pm 1$$

sarà diverso da zero [per la irriducibilità della $f(x)$], e diverso anche da ± 1, se pure escludiamo per q quegli *eventuali* valori (in numero finito) che rendessero $f(q\mu) = \pm 1$. Così il numero N avrà almeno un divisore primo p, che non dividerà μ, risultando dalla (16)

$$N \equiv \pm 1 \qquad (\mathrm{mod}\,\mu),$$

e per questo numero primo p la congruenza

$$(17) \qquad f(\xi) \equiv 0 \qquad (\mathrm{mod}\,p)$$

avrà almeno la radice $\xi = q\mu$. C. D. D.

In questo risultato poniamo $\mu = C$, essendo C l'indice di θ, e la (17) avrà una radice ξ, mentre il modulo p è primo con C. A questa radice ξ corrisponderà (n° 7) un ideale P primo e di primo grado, divisore di p ($NP = p$). Ma ora si vede subito che di questi numeri primi p, che non dividono C e pei quali è solubile la congruenza (17), se ne dànno infiniti. E difatti, per quanti di tali numeri primi si sieno già trovati, diciamo

$$p_1, \quad p_2, \quad \ldots, \quad p_r,$$

se nel teorema dimostrato poniamo

$$\mu = C p_1 p_2 \ldots p_r,$$

ne troveremo uno nuovo p, che non divide C ed è diverso da $p_1, p_2, \ldots, p_r$. L'infinità degli ideali primi di primo grado in $k(\theta)$ risulta così manifesta.

9. Terminiamo la presente Nota colla ricerca del *carattere quadratico* di un qualunque intero ω del corpo $k(\theta)$ rispetto ad un ideale primo P di *primo grado* che non entra in ω, e nemmeno nel numero

primo 2 (¹). Col simbolo di Dirichlet $\left[\frac{\omega}{\mathrm{P}}\right]$ indichiamo l'unità positiva o negativa, secondo che ω è residuo quadratico o non residuo (mod P), cioè secondo che è solubile, ovvero insolubile la congruenza

$$x^2 \equiv \omega \pmod{\mathrm{P}}. \tag{18}$$

Dimostriamo che il calcolo del simbolo $\left[\frac{\omega}{\mathrm{P}}\right]$ si riduce a quello di un simbolo di Legendre $\left(\frac{r}{p}\right)$, dove p è il numero primo (dispari) norma di P.

Nel caso attuale $\mathrm{NP} = p$ formano già un sistema completo di resti (mod P) i p numeri razionali

$$0, \quad 1, \quad 2, \quad \ldots, \quad p-1,$$

poichè un numero razionale r che sia $\equiv 0 \pmod{\mathrm{P}}$ è necessariamente multiplo del più piccolo p, cioè è anche $r \equiv 0 \pmod{p}$. Per esaminare se la congruenza (18) è solubile, si può già supporre ω sostituito col numero razionale $r \not\equiv 0 \pmod{p}$, a cui ω è congruo (mod P), ed anche pel valore dell' incognita x si può assumere un numero razionale ξ.

Secondo le osservazioni superiori, la congruenza (18) equivale così perfettamente all' altra di aritmetica razionale

$$\xi^2 \equiv r \pmod{p};$$

ne segue: *Se r è un numero razionale (non divisibile per p) si ha*

$$\left[\frac{r}{\mathrm{P}}\right] = \left(\frac{r}{p}\right). \tag{19}$$

Ciò premesso, sia dato un qualunque intero ω in $k(\theta)$

$$\omega = h_1 + h_2\omega_2 + \ldots + h_n\omega_n,$$

e prendiamo la base di P sotto la forma del n° 5

$$\mathrm{P} = [p, \omega_2 - \xi_2, \ldots, \omega_n - \xi_n].$$

Per calcolare $\left[\frac{\omega}{\mathrm{P}}\right]$ basterà determinare il numero razionale

(¹) Se P divide 2, *qualunque* intero ω è suo residuo quadratico.

$r \equiv \omega \pmod{\mathrm{P}}$, ed applicare quindi la (19). Ora, dovendosi avere

$$h_1 + h_2\omega_2 + \ldots + h_n\omega_n = r + p x_1 + (\omega_2 - \xi_2)x_2 + \ldots + (\omega_n - \xi_n)x_n,$$

dove $x_1, x_2, \ldots, x_n$ sono interi razionali, ne deduciamo

$$x_2 = h_2, \qquad x_3 = h_3, \qquad \ldots, \qquad x_n = h_n,$$

indi

$$r = h_1 + h_2\xi_2 + h_3\xi_3 + \ldots + h_n\xi_n.$$

Così resta stabilità la formola

$$\left[\frac{h_1 + h_2\omega_2 + \ldots + h_n\omega_n}{\mathrm{P}}\right] = \left(\frac{h_1 + h_2\xi_2 + \ldots + h_n\xi_n}{p}\right), \tag{20}$$

che effettua la riduzione del simbolo $\left[\frac{\omega}{\mathrm{P}}\right]$ ad un simbolo di Legendre. Nel caso del corpo quadratico di Gauss $k(\sqrt{-1})$, quando per P si assuma un fattore primo complesso π del numero primo $p \equiv 1 \pmod 4$, la (20) diventa una ben nota formola di Dirichlet.