ATTI

DELLA

REALE ACCADEMIA NAZIONALE DEI LINCEI

ANNO CCCXIX.

1922

SERIE QUINTA

RENDICONTI

Classe di scienze fisiche, matematiche e naturali.

VOLUME XXXI.

2° SEMESTRE.

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA NAZIONALE DEI LINCEI

PROPRIETÀ DEL DOTT. PIO BEFANI

1922

RENDICONTI

DELLE SEDUTE

DELLA REALE ACCADEMIA NAZIONALE DEI LINCEI

Classe di scienze fisiche, matematiche e naturali.

Seduta del 5 novembre 1922.

V. Volterra, Vicepresidente.

MEMORIE E NOTE DI SOCI

Matematica. — *Dimostrazione elementare della infinità degli ideali primi di primo grado in ogni corpo algebrico.* Nota del Socio Luigi Bianchi.

Il teorema enunciato nel titolo di questa nota si suole dimostrare ricorrendo ai principii dell'aritmetica analitica [1]. In occasione di una mia ricerca sugli ideali primarî assoluti in un corpo algebrico [2], ho osservato che la proprietà si può stabilire elementarmente in casi assai estesi, quando p. e. il corpo algebrico è totalmente reale (reale con tutti i suoi coniugati). Scopo delle seguenti semplicissime considerazioni è di liberare la detta dimostrazione elementare da ogni restrizione ed ottenere così il teorema in tutta generalità.

Per questo stabiliremo, con procedimento euclideo, la seguente proposizione d'aritmetica razionale:

A) Se

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

è un polinomio razionale intero a coefficienti interi, esistono infiniti numeri primi p pei quali la congruenza

$$f(x) \equiv 0 \pmod{p} \tag{I}$$

ammette almeno una radice [3].

[1] Cfr. p. e. Weber, *Algebra*, 2e Auflage, IIer Bd. S. 727.

[2] *Journal de Mathém*, 8e série, t. V, 1922.

[3] Il teorema (*A*) (colla restrizione superflua che $f(x)$ sia irriducibile) è dedotto, in una recente Memoria di Rados (*Math. Annalen.*, Bd. 87, S. 83), come conseguenza di un notevole teorema di Kronecker [sulla frequenza dei numeri primi p pei quali ammette soluzioni la (I)] appartenente all'aritmetica analitica.

Nel caso $a_n = 0$ la proprietà è evidente, poichè allora, per *qualunque* numero primo p, la (I) ammette la radice $x \equiv 0 \pmod{p}$; supponiamo quindi $a_n \neq 0$. Fissati r numeri primi diversi qualunque

$$(1) \qquad p_1, p_2, \cdots, p_r,$$

indichiamo con

$$(2) \qquad m = p_1 p_2 \cdots p_r$$

il loro prodotto, e diamo alla x un valore intero divisibile pel prodotto ma_n, sia

$$x = ma_n \,.\, h,$$

con h razionale intero arbitrario. La $f(x)$ assumerà il valore

$$f(ma_n h) = a_n \{a_0 m^n a_n^{n-1} h^n + a_1 m^{n-1} a_n^{n-2} h^{n-1} + \cdots + a_{n-1} mh + 1\},$$

ovvero, posto

$$\mathrm{N} = a_0 m^n a_n^{n-1} h^n + a_1 m^{n-1} a_n^{n-2} h^{n-1} + \cdots + a_{n-1} mh + 1,$$

$$(3) \qquad f(ma_n h) = a_n \,.\, \mathrm{N},$$

e sarà

$$(4) \qquad \mathrm{N} \equiv 1 \pmod{m}.$$

Questo intero N, non nullo, potrà eventualmente risultare $= \pm 1$ per un numero finito di valori di h, che intenderemo evitati. Così N, risultando in valore assoluto > 1, ammetterà almeno un divisore primo p, il quale sarà diverso dagli r numeri primi (1), poichè per uno qualunque p_i di questi si ha per la (4)

$$(4) \qquad \mathrm{N} \equiv 1 \pmod{p_i}.$$

Così, per quanti numeri primi siansi già fissati, esiste un ulteriore numero primo p, pel quale la congruenza (I) ammette almeno una radice: e il teorema A) risulta stabilito.

Abbiasi ora un qualunque corpo algebrico $\mathrm{K}(\theta)$, di grado n, di cui sia θ un numero intero generatore, soddisfacente all'equazione *irriducibile* di grado n

$$(5) \qquad f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0,$$

con primo coefficiente $a_0 = 1$ e i rimanenti razionali interi. Scelta una base *minima* del corpo, sia

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

le potenze $1, \theta, \theta^2, \cdots, \theta^{n-1}$ di θ si esprimono per gli interi ω_i della base mediante una sostituzione lineare a coefficienti interi c_{ik} del tipo

$$(6) \quad \begin{cases} 1 &= c_{11}\,\omega_1 + c_{12}\,\omega_2 + \cdots + c_{1n}\,\omega_n \\ \theta &= c_{21}\,\omega_1 + c_{22}\,\omega_2 + \cdots + c_{2n}\,\omega_n \\ \theta^2 &= c_{31}\,\omega_1 + c_{32}\,\omega_2 + \cdots + c_{3n}\,\omega_n \\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \theta^{n-1} &= c_{n1}\,\omega_1 + c_{n2}\,\omega_2 + \cdots + c_{nn}\,\omega_n\,. \end{cases}$$

Il modulo C di questa sostituzione, cioè il determinante

$$C = |c_{ik}|,$$

il cui quadrato eguaglia il quoziente del discriminante di θ pel numero fondamentale D del corpo, è detto da Dedekind [1] l'indice dell'intero θ nel corpo $K(\theta)$, e Dedekind ha dimostrato che, *se un numero primo p non divide l'indice C di θ*, la risoluzione del numero primo p nei suoi fattori ideali primi si ottiene, con procedimento razionale, decomponendo, rispetto al modulo p, il polinomio intero $f(x)$ nei suoi fattori irriducibili (m. c. § 2). In particolare, ed è questo il caso che a noi qui interessa, se il numero primo p non divide C e la congruenza

$$f(x) \equiv 0 \pmod{p}$$

ammette una radice ξ, l'ideale P massimo comun divisore dei due interi

$$p\,,\ \theta - \xi$$

ha la sua norma $= p$, $NP = p$, ed è quindi un ideale primo di primo grado, divisore di p.

Dal teorema *A*) segue l'esistenza di *infiniti* numeri primi p, che non dividono C, e per ciascuno dei quali la congruenza (I) ammette almeno una radice, onde si conclude:

B) *In ogni corpo algebrico* $K(\theta)$ *esistono infiniti ideali primi di primo grado.*

Terminiamo coll'osservare che, se si prende in particolare per $K(\theta)$ il corpo di grado $\varphi(m)$ delle radici m^{me} dell'unità (m qualunque), assumendo per θ una radice primitiva m^{ma}, l'indice C è $= 1$, e pel risultato classico di Kummer gli ideali primi di primo grado in $K(\theta)$ sono tutti e soli i divisori dei numeri primi p che sono $\equiv 1 \pmod{m}$. La dimostrazione elementare esposta si cangia quindi in quella ben nota colla quale si prova che la progressione aritmetica $mx + 1$ contiene infiniti numeri primi [2].

(1) *Ueber den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen* (Abhandlungen der Göttinger Gesellschaft 23er Bd. 1878).

(2) V. p. e. Kronecker, *Vorlesungen über Zahlentheorie*, Ier Bd. S. 440-441.