A Theorem on the Relative Norm of an Ideal.

A Theorem on the Relative Norm of an Ideal

By LADISLAS FUCHS in Budapest

From the theory of the algebraic numbers it is well known that for the norm of an ideal the following theorem holds[1]):

Supposing that $\mathfrak{a}$ *is an ideal in an over-field of degree* n *of the field of the rational numbers, and* $(\alpha_1, \ldots, \alpha_n)$ *is a basis of* $\mathfrak{a}$ *and* $(\omega_1, \ldots, \omega_n)$ *is that of the unit ideal* $\mathfrak{o}$ *with respect to the rational integers, then*[2])

$$\left| \begin{matrix} \alpha_1^{(1)} \ldots \alpha_1^{(n)} \\ \cdots\cdots \\ \alpha_n^{(1)} \ldots \alpha_n^{(n)} \end{matrix} \right|^2 = N(\mathfrak{a})^2 \left| \begin{matrix} \omega_1^{(1)} \ldots \omega_1^{(n)} \\ \cdots\cdots \\ \omega_n^{(1)} \ldots \omega_n^{(n)} \end{matrix} \right|^2$$

denoting by $N(\mathfrak{a})$ *the norm of* $\mathfrak{a}$ *defined*[3]) *as the number of the classes incongruent mod* $\mathfrak{a}$.

In the present paper we intend to give the proof of an entirely analogous theorem on the relative norm of an ideal.

The proof in whole generality presents difficulties and complications which do not arise in the case of the rational numbers. Namely, in the general case the ideals may have their basis containing elements in number more than the degree n of the over-field, and therefore, the basis-elements of the unit ideal and those of the over-field are different ones. Essentially, however, the method of Hilbert[4]) will be applied even to the general case, but in a far-reaching generality.

In demonstrating the truth of the generalized theorem stated at the end of the present paper the first step is the introduction of the ideals $\mathfrak{R}_e(\mathfrak{a})$. Now we have to take into account that the ideals $\mathfrak{R}_l(\mathfrak{o})$ need not be necessarily equal to the unit ideal; this would be the case only if the basis of $\mathfrak{o}$ would be at the same time a basis of the over-field, so e. g. in the case of the rational numbers.

[1]) See *Hecke* [1], theorem 76, p. 98; *Hilbert* [1], § 7, theorem 19; *Landau* [1], theorem 103, p. 31. The works referred to are given at the end of the present paper.

[2]) $\alpha^{(\kappa)}$ denote the conjugates of α. The square of the determinant $\left|\omega_i^{(\kappa)}\right|$ standing on the right side of the equation is called the discriminant of the over-field.

[3]) The definition of the ideal-norm is due to Dedekind, see *Dedekind* [1], p. 564.

[4]) See *Hilbert* [1].

Then, for the sake of brief expressibility the definition of an array-ideal of n columns and of more than or just n rows is given. The notion of the array-ideal can be considered as a generalization of a principal ideal with a determinant as basis to the case if the ring is not a principal-ideal-ring.

After these we shall discuss the product of the ideals $\mathfrak{R}_l(\mathfrak{a})$ and give a representation of it as an array-ideal $\mathfrak{R}(\mathfrak{a})$ made up of coefficients determined by the basis of $\mathfrak{a}$. This representation is of much importance, for it involves the possibility of the proof of $\frac{\mathfrak{R}(\mathfrak{a})}{\mathfrak{R}(\mathfrak{o})} = \mathfrak{M}(\mathfrak{a})$ depending on $\mathfrak{a}$, but neither on the basis of $\mathfrak{a}$ nor on that of the over-field.

The following step is to give for $\mathfrak{M}(\mathfrak{a})$ in a certain sense similar representation to that of $N(\mathfrak{a})$ in the quoted theorem; namely, $\mathfrak{M}(\mathfrak{a})$ will be proved to be expressible as the quotient of two array-ideals made up of the conjugates of the basis-elements of $\mathfrak{a}$ and $\mathfrak{o}$. After proving that $\mathfrak{M}(\mathfrak{a})$ and the Hilbertian relative norm $\mathfrak{N}(\mathfrak{a})$ have the same norm, we shall justify the identity of $\mathfrak{M}(\mathfrak{a})$ and $\mathfrak{N}(\mathfrak{a})$ by showing that $\mathfrak{N}(\mathfrak{a})$ is a multiple of $\mathfrak{M}(\mathfrak{a})$. And this will complete the proof.

Be the fundamental domain Σ a five-axioms-ring[5]), i. e., a ring in which the principal theorem of the theory of ideals holds: every ideal $\mathfrak{A}$ other than (0) is the product of uniquely determined prime-ideal-powers. It is further assumed that the residue-class-ring $\Sigma/\mathfrak{A}$ [$\mathfrak{A}$ different from (0)] consists only of a finite number of elements[6]).

We shall denote by Ω the quotient-field of Σ and by P a separable algebraic over-field of degree n of Ω. Let further Γ be the ring of the integral elements of P with respect to Σ. The principal theorem of the theory of ideals holds, of course, even in Γ.

In the field P there exist n linearly independent elements,

$$\omega_1, \ldots, \omega_n$$

such that every element of P can be uniquely expressed as a linear combination of ω_i with coefficients in Ω, i. e., in the form[7])

$$\omega = \sum_{i=1}^{n} a_i \, \omega_i \qquad (a_i \, \varepsilon \, \Omega).$$

[5]) *E. Noether* proved (see her paper [1]) that the principal theorem of the theory of ideals is equivalent to five axioms: 1) the maximal condition, 2) the minimal condition 3) the existence of a unit element, 4) deficiency of divisors of zero, 5) the ring being integrally-closed in its quotient-field. All of these axioms will be made use.

[6]) The number of the elements of $\Sigma/\mathfrak{A}$ will be called as usual the (absolute) norm of $\mathfrak{A}$.

[7]) See *Waerden* [1], p. 107.

The system ω_i is said to be a *basis of* P with respect to Ω. Although the order of the basis-elements is irrelevant, we shall speak about an *ordered basis of* P understanding a set of basis-elements given together with their order.

Consider all the elements of an ideal $\mathfrak{a}$ which are of the type

$$\alpha = \sum_{i=1}^{l} r_i \omega_i \qquad (1 \leqslant l \leqslant n \; ; \quad r_i \varepsilon \Omega) \; .$$

The l^{th} coefficients r_e form an ideal of Σ, which will be denoted by $\mathfrak{R}_l(\mathfrak{a})$. Indeed[8]), the difference of two r_l, and the product of an r_l with an element of Σ belong also to the set of the r_l, further there exists in Σ an element d differing from 0 such that the elements of $d \cdot \mathfrak{R}_l(\mathfrak{a})$ are already contained in Σ[9]).

That $\mathfrak{a} \neq (0)$ implies $\mathfrak{R}_l(\mathfrak{a}) \neq (0)$ we wish to prove immediately. The field P has certainly an element ω of the form

$$\omega = \sum_{i=1}^{l} t_i \omega_i \qquad\qquad (t_l \neq 0) \; .$$

An element $g \neq 0$ of Σ and an element $a \neq 0$ of $\mathfrak{a}$ can always be chosen to be $g\omega$ in Γ[10]) and a in Σ respectively; thus $ag\omega$ is contained in $\mathfrak{a}$, i. e., $\mathfrak{a}$ has an element α of the form

$$\alpha = \sum_{i=1}^{l} (a g t_i) \, \omega_i \; ,$$

where $agt_l \neq 0$, Σ having no divisor of zero. This means, $\mathfrak{R}_l(\mathfrak{a})$ has a non-vanishing element, which proves the statement.

The above process shows that any ideal $\mathfrak{a}$ in Γ has n corresponding ideals in Σ, namely

$$\mathfrak{R}_1(\mathfrak{a}), \ldots, \mathfrak{R}_n(\mathfrak{a}) \; ,$$

none of which is equal to (0). In particular, the ideals corresponding to the unit ideal $\mathfrak{o}$ are $\mathfrak{R}_1(\mathfrak{o}), \ldots, \mathfrak{R}_n(\mathfrak{o})$. The ideals $\mathfrak{R}_l(\mathfrak{a})$ are uniquely determined by the ideal $\mathfrak{a}$ and by the ordered basis of P at the same time.

---

8) The $\mathfrak{R}_l(\mathfrak{a})$ are not necessarily integral ideals. — We have only to prove that $\mathfrak{R}_l(\mathfrak{a})$ is a module with a finite basis; see *Hecke* [1], p. 113 and also *Waerden* [2], p. 91.

9) The proof of the existence of such a d runs by a similar reasoning to that of e. g. *Waerden* [2], pp. 80—81; take for instance $d = \Delta^2(\omega_1, \ldots, \omega_n) = \left| \omega_i^{(k)} \right|^2$.

10) See *Waerden* [2], p. 80.

We observe that $\mathfrak{b} \equiv 0(\mathfrak{a})$ implies

$$\mathfrak{R}_\iota(\mathfrak{b}) \equiv 0(\mathfrak{R}_\iota(\mathfrak{a})) .$$

This remark need not be proved, because it is from the construction evident. As a consequence of this we get the congruence

$$\mathfrak{R}_\iota(\mathfrak{a}) \equiv 0(\mathfrak{R}_\iota(\mathfrak{o})) \tag{1}$$

holding for any ideal $\mathfrak{a}$ of Γ.

Without restricting the generality we may assume that the ideals $\mathfrak{R}_\iota(\mathfrak{o})$ are integral. This case being simply a matter of convenience can be reached by a suitable choosing of $\omega_1, \ldots, \omega_n$. Then, for every $\mathfrak{a}$, $\mathfrak{R}_\iota(\mathfrak{a})$ are also integral.

Now remember the well-known fact that any ideal $\mathfrak{a}$ of Γ has a basis consisting of the elements of the type[11])

$$\begin{aligned}
&\alpha_1 = r_{11}\,\omega_1 \\
&\cdots\cdots\cdots \\
&\alpha_{\mu_1} = r_{\mu_1 1}\,\omega_1 \\
&\alpha_{\mu_1+1} = r_{\mu_1+1,1}\,\omega_1 + r_{\mu_1+1,2}\,\omega_2 \\
&\cdots\cdots\cdots\cdots\cdots\cdots \qquad\qquad (r_{\mu i}\,\varepsilon\,\Omega) \\
&\alpha_{\mu_2} = r_{\mu_2 1}\,\omega_1 + r_{\mu_2 2}\,\omega_2 \\
&\cdots\cdots\cdots\cdots\cdots \\
&\alpha_{\mu_{n-1}+1} = r_{\mu_{n-1}+1,1}\,\omega_1 + \cdots + r_{\mu_{n-1}+1,n}\,\omega_n \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\alpha_M = r_{M1}\,\omega_1 + \cdots\cdots + r_{Mn}\,\omega_n .
\end{aligned} \tag{2}$$

Every element α of $\mathfrak{a}$ is linearly expressible by means of these basis-elements with coefficients in Σ, i. e., α is of the form

$$\alpha = \sum_{\mu=1}^{M} a_\mu\,\alpha_\mu \qquad (a_\mu\,\varepsilon\,\Sigma) .$$

In consequence of the definition of $\mathfrak{R}_n(\mathfrak{a})$, the basis-elements of $\mathfrak{R}_n(\mathfrak{a})$ are evidently $r_{\mu_{n-1}+1,n}, \ldots, r_{Mn}$, that is to say,

$$\mathfrak{R}_n(\mathfrak{a}) = (r_{\mu_{n-1}+1,n}, \ldots, r_{Mn}) .$$

---

[11]) For the statement in this general form, cf. *Waerden* [2], pp. 75—76; in the special case if Σ is the principal-ideal-ring of the rational integers, see also *Hecke* [1], p. 41 and *Landau* [1], p. 30; [2], p. 117.

We have similarly

$$\mathfrak{R}_{n-1}(\mathfrak{a}) = (r_{\mu_{n-2}+1,\,n-1}, \ldots, r_{\mu_{n-1}\cdot\, n-1}) ,$$

etc., finally

$$\mathfrak{R}_1(\mathfrak{a}) = (r_{11}, \ldots r_{\mu_1 1}) .$$

Before going to examine the product of the ideals $\mathfrak{R}_1(\mathfrak{a}),\ldots,\mathfrak{R}_n(\mathfrak{a})$, we define the notion of an array-ideal; this will simplify somewhat our statements.

The ideal, the basis-elements of which are all the determinants of order n exhibited by the matrix

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ a_{N1} & a_{N2} & \ldots & a_{Nn} \end{pmatrix} \qquad (N \geqslant n)$$

will be called an *array-ideal* and denoted by two parentheses: $((a_{\nu i}))$. We shall deal only with array-ideals consisting of n columns and of at least n rows.

Now, it is easy to show that any basis-element of $\mathfrak{R}_1(\mathfrak{a})\ldots\mathfrak{R}_n(\mathfrak{a})$ can be found among the basis-elements of the array-ideal

$$\mathfrak{R}(\mathfrak{a}) = \left(\!\!\left(\begin{matrix} r_{11} & & & \\ \vdots & & & \\ r_{\mu_1 1} & & & \\ r_{\mu_1+1,1} & r_{\mu_1+1,2} & & \\ \cdot & \cdot & \cdot & \cdot \\ r_{\mu_2 1} & r_{\mu_2 2} & & \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ r_{M1} & r_{M2} & \ldots & r_{Mn} \end{matrix}\right)\!\!\right) \tag{3}$$

made up of the coefficients of ω_i in (2). In fact, the basis-elements of $\mathfrak{R}_1(\mathfrak{a})\ldots\mathfrak{R}_n(\mathfrak{a})$ are just the determinants of order n having their first row among the rows $1,\ldots,\mu_1$, their second row among the rows $\mu_1+1,\ldots,\mu_2$, etc., finally, their n^{th} row among the rows $\mu_{n-1}+1,\ldots,M$ of the matrix of the array-ideal $\mathfrak{R}(\mathfrak{a})$. Moreover, we can state the following theorem.

Theorem 1. The array-ideal $\mathfrak{R}(\mathfrak{a})$ *is equal to the product* $\mathfrak{R}_1(\mathfrak{a})\ldots\mathfrak{R}_n(\mathfrak{a})$.

It will clearly be sufficient to prove that any basis-element of the array-ideal in question is contained in $\mathfrak{R}_1(\mathfrak{a})\ldots\mathfrak{R}_n(\mathfrak{a})$.

Now assume that every determinant of order $\kappa - 1$ containing only elements of the last $\kappa - 1$ columns of the matrix of the array-ideal $\mathfrak{R}(\mathfrak{a})$ is an element of the ideal $\mathfrak{R}_{n-\kappa+2}(\mathfrak{a})\ldots\mathfrak{R}_n(\mathfrak{a})$, i. e.,

$$\begin{vmatrix} r_{p_1,\, n-\kappa+2} \cdots r_{p_1 n} \\ \cdots\cdots\cdots\cdots \\ r_{p_{\kappa-1},\, n-\kappa+2} \cdots r_{p_{\kappa-1} n} \end{vmatrix} \equiv 0\left(\mathfrak{R}_{n-\kappa+2}(\mathfrak{a})\ldots\mathfrak{R}_n(\mathfrak{a})\right) ,$$

anyhow the subscripts $p_1, \ldots, p_{\kappa-1}$ are chosen from $1, \ldots, M$. We have this statement in the case of $\kappa = 2$ quite clear. Be

$$R = \begin{vmatrix} r_{i_1,\, n-\kappa+1} \cdots r_{i_1, n} \\ \cdots\cdots\cdots\cdots \\ r_{i_\kappa,\, n-\kappa+1} \cdots r_{i_\kappa, n} \end{vmatrix}$$

any determinant consisting of elements occuring in the last κ columns of the matrix in question and let the elements x_q be chosen to satisfy the following system of homogeneous linear equations

$$\begin{aligned} r_{i_1, n} x_1 + \cdots + r_{i_\kappa n} x_\kappa &= 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ r_{i_1, n-\kappa+2}\, x_1 + \cdots + r_{i_\kappa, n-\kappa+2}\, x_\kappa &= 0 . \end{aligned} \tag{4}$$

The x_q will be more specified later.

Now we have to take into account that in

$$\alpha = \alpha_{i_1}\, x_1 + \cdots + \alpha_{i_n}\, x_n$$

the coefficients of $\omega_{n-\kappa+2}, \ldots, \omega_n$ are zeros, therefore, by definition, the coefficient of $\omega_{n-\kappa+1}$ is an element of $\mathfrak{R}_{n-\kappa+1}(\mathfrak{a})$:

$$r_{i_1,\, n-\kappa+1} x_1 + \cdots + r_{i_\kappa, n-\kappa+1} x_\kappa \equiv 0 \qquad (\mathfrak{R}_{n-\kappa+1}(\mathfrak{a})) \tag{5}$$

From the above system of equations for x_q we obtain as solution the ratio

$$x_1 : \ldots : x_\kappa = R_1 : \ldots : R_\kappa ,$$

R_q being the first minor in R belonging to $r_{i_q, n-\kappa+1}$.

The ideals $\mathfrak{K}_q$ of Σ may be taken to satisfy the conditions

$$\text{A)} \quad R_1 : \ldots : R_\kappa = \mathfrak{K}_1 : \ldots : \mathfrak{K}_\kappa$$

and

$$\text{B)} \quad (\mathfrak{K}_1, \ldots, \mathfrak{K}_\kappa) = (1) = \mathfrak{O} \; .$$

Let further $\mathfrak{G} \neq (0)$ be subject to the postulates[12])

I) $(\mathfrak{G}, \mathfrak{R}_{n-\kappa+1}(\mathfrak{a}) \ldots \mathfrak{R}_n(\mathfrak{a})) = \mathfrak{O}$.

II) *for one and hence for all* q: $\mathfrak{G} \cdot \mathfrak{K}_q$ *is a principal ideal,* $\mathfrak{G} \cdot \mathfrak{K}_q = (x_q)$.

These x_q satisfy the equations (4), so, from the hypothesis of R_q being contained in $\mathfrak{R}_{n-\kappa+2}(\mathfrak{a}) \ldots \mathfrak{R}_n(\mathfrak{a})$, on using (5) we easily see that

$$R_q \cdot r_{i_1, n-\kappa+1} x_1 + \cdots + R_q \cdot r_{i_\kappa, n-\kappa+1} x_\kappa \equiv 0 \;\; (\mathfrak{R}_{n-\kappa+1}(\mathfrak{a}) \ldots \mathfrak{R}_n(\mathfrak{a})) \quad (6)$$

Remember that the equality

$$R_q \cdot x_{q'} = x_q \cdot R_{q'}$$

holds by giving q and q' any values out of $1, \ldots, \kappa$. Thus we may write

$$x_q(R_1 r_{i_1, n-\kappa+1} + \cdots + R_\kappa r_{i_\kappa, n-\kappa+1}) = x_q \cdot R \equiv 0 \;\; (\mathfrak{R}_{n-\kappa+1}(\mathfrak{a}) \ldots \mathfrak{R}_n(\mathfrak{a}))$$

involving that also

$$\mathfrak{G} \cdot R = (x_1, \ldots, x_\kappa) \cdot R \equiv 0 \;\; (\mathfrak{R}_{n-\kappa+1}(\mathfrak{a}) \ldots \mathfrak{R}_n(\mathfrak{a})) \; .$$

Now recall that $\mathfrak{G}$ was chosen to have no common divisor with $\mathfrak{R}_{n-\kappa+1}(\mathfrak{a}) \ldots \mathfrak{R}_n(\mathfrak{a})$, therefore the last congruence requires

$$R \equiv 0 \;\; (\mathfrak{R}_{n-\kappa+1}(\mathfrak{a}) \ldots \mathfrak{R}_n(\mathfrak{a})) \; .$$

This completes the proof of theorem 1.

We pass now to the proof of

Theorem 2. Supposing that

$$\alpha_\mu = \sum_{i=1}^{n} r_{\mu i} \, \omega_i \qquad (\mu = 1, \ldots, M \, ; \;\; r_{\mu i} \in \Omega)$$

is a basis of the ideal $\mathfrak{a}$; *the array-ideal*

$$\mathfrak{R}(\mathfrak{a}) = \left(\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ r_{M1} & \cdots & r_{Mn} \end{pmatrix} \right)$$

is independent of the basis of $\mathfrak{a}$.

[12]) See *Waerden* [2], p. 90.

Indeed, employ

$$\alpha_\sigma^* = \sum_{i=1}^{n} r_{\sigma i}^* \omega_i \qquad (\sigma = 1, \ldots, S \, ; \quad r_{\sigma i}^* \, \varepsilon \, \Omega)$$

as a basis of $\mathfrak{a}$ in place of α_μ and use the familiar fact that the two systems α_μ and α_σ^* are related by such linear equations:

$$\alpha_\sigma^* = \sum_{\mu=1}^{M} c_{\sigma\mu} \, \alpha_\mu = \sum_{i=1}^{n} \Big(\sum_{\mu=1}^{M} c_{\sigma\mu} r_{\mu i} \Big) \omega_i \quad (\sigma = 1, \ldots, S \, ; \; c_{\sigma\mu} \, \varepsilon \, \Sigma) \, .$$

Therefore

$$\sum_{\mu=1}^{M} c_{\sigma\mu} \, r_{\mu i} = r_{\sigma i}^* \, .$$

A basis-element of the array-ideal $\mathfrak{R}^*(\mathfrak{a})$ is evidently[13])

$$\begin{vmatrix} r_{\sigma_1 1}^* & \cdots & r_{\sigma_1 n}^* \\ \cdots & \cdots & \cdots \\ r_{\sigma_n 1}^* & \cdots & r_{\sigma_n n}^* \end{vmatrix} = \begin{vmatrix} \sum\limits_{\mu=1}^{M} c_{\sigma_1 \mu} \, r_{\mu 1} & \cdots & \sum\limits_{\mu=1}^{M} c_{\sigma_1 \mu} \, r_{\mu n} \\ \cdots & \cdots & \cdots \\ \sum\limits_{\mu=1}^{M} c_{\sigma_n \mu} \, r_{\mu 1} & \cdots & \sum\limits_{\mu=1}^{M} c_{\sigma_n \mu} \, r_{\mu n} \end{vmatrix} =$$

$$= \begin{pmatrix} c_{\sigma_1 1} & \cdots & c_{\sigma_n 1} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ c_{\sigma_1 M} & \cdots & c_{\sigma_n M} \end{pmatrix} \cdot \begin{pmatrix} r_{11} & \cdots & r_{M1} \\ \cdots & \cdots & \cdots \\ r_{1n} & \cdots & r_{Mn} \end{pmatrix} =$$

$$= \sum_{1 \leqslant \mu \leqslant M} \begin{vmatrix} c_{\sigma_1 \mu_1} & \cdots & c_{\sigma_n \mu_1} \\ \cdots & \cdots & \cdots \\ c_{\sigma_1 \mu_n} & \cdots & c_{\sigma_n \mu_n} \end{vmatrix} \cdot \begin{vmatrix} r_{\mu_1 1} & \cdots & r_{\mu_n 1} \\ \cdots & \cdots & \cdots \\ r_{\mu_1 n} & \cdots & r_{\mu_n n} \end{vmatrix}$$

the summation being extended over all possible combinations of the subscripts μ. The determinants

$$\begin{vmatrix} r_{\mu_1 1} & \cdots & r_{\mu_n 1} \\ \cdots & \cdots & \cdots \\ r_{\mu_1 n} & \cdots & r_{\mu_n n} \end{vmatrix}$$

offer just the basis-elements of $\mathfrak{R}(\mathfrak{a})$, consequently, the basis-elements of $\mathfrak{R}^*(\mathfrak{a})$ are contained in $\mathfrak{R}(\mathfrak{a})$, i. e.,

$$\mathfrak{R}^*(\mathfrak{a}) \equiv 0 \, (\mathfrak{R}(\mathfrak{a})) \, .$$

---

[13]) Cf. *G. Kowalewski*, Determinantentheorie, p. 72.

Changing the roles of $\mathfrak{R}^*(\mathfrak{a})$ and $\mathfrak{R}(\mathfrak{a})$, the same reasoning shows that also

$$\mathfrak{R}(\mathfrak{a}) \equiv 0 \; (\mathfrak{R}^*(\mathfrak{a})) \; .$$

The two last congruences give together the equality

$$\mathfrak{R}(\mathfrak{a}) = \mathfrak{R}^*(\mathfrak{a}) \; , \qquad \text{q. e. d.}$$

Combining the theorems 1 and 2 we have the result that any array-ideal $\mathfrak{R}(\mathfrak{a})$ is just equal to the idealproduct $\mathfrak{R}_1(\mathfrak{a})\ldots\mathfrak{R}_n(\mathfrak{a})$. In particular, denoting by

$$o_\nu = \sum_{i=1}^{n} s_{\nu i}\,\omega_i \qquad (\nu = 1,\ldots,N\,; \;\; s_{\nu i}\,\varepsilon\,\Omega)$$

a basis of the unit ideal $\mathfrak{o}$, the array-ideal

$$\mathfrak{R}(\mathfrak{o}) = \left(\left(\begin{array}{c} s_{11}\;\ldots\;s_{1n} \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ s_{N1}\ldots s_{Nn} \end{array}\right)\right)$$

is always equal to $\mathfrak{R}_1(\mathfrak{o})\ldots\mathfrak{R}_n(\mathfrak{o})$.

Next we introduce another system of linearly independent basis-elements,

$$\omega_1', \ldots, \omega_n',$$

in place of $\omega_1,\ldots,\omega_n$, and denote by $\mathfrak{R}'(\mathfrak{a})$ the array-ideal corresponding to $\mathfrak{R}(\mathfrak{a})$.

The two systems of basis-elements are connected by the equations

$$\omega_i = \sum_{j=1}^{n} b_{ij}\,\omega_j' \qquad (i = 1,\ldots,n\,; \;\; b_{ij}\,\varepsilon\,\Omega)\,,$$

where the determinant

$$b = \left|\begin{array}{c} b_{11}\ldots b_{1n} \\ \ldots\ldots\ldots \\ b_{n1}\ldots b_{nn} \end{array}\right|$$

differs from 0[14]).

[14]) If the elements ω_j' are a permutation of ω_i, then there exist also equations of this kind and the determinant b is equal to 1 or to -1.

Since the basis-elements of $\mathfrak{a}$ are of the form

$$\alpha_\mu = \sum_{j=1}^{n} r'_{\mu j}\, \omega'_j$$

and at the same time of the form

$$\alpha_\mu = \sum_{i=1}^{n} r_{\mu i}\, \omega_i = \sum_{j=1}^{n} \Big(\sum_{i=1}^{n} r_{\mu i} b_{ij}\Big)\, \omega'_j \;,$$

we have

$$r'_{\mu j} = \sum_{i=1}^{n} r_{\mu i}\, b_{ij} \;.$$

Thus a basis-element of $\mathfrak{R}'(\mathfrak{a})$ is

$$\begin{vmatrix} r'_{\mu_1 1} & \cdots & r'_{\mu_1 n} \\ \cdots & \cdots & \cdots \\ r'_{\mu_n 1} & \cdots & r'_{\mu_n n} \end{vmatrix} = \begin{vmatrix} r_{\mu_1 1} & \cdots & r_{\mu_n 1} \\ \cdots & \cdots & \cdots \\ r_{\mu_1 n} & \cdots & r_{\mu_n n} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & \cdots & b_{n1} \\ \cdots & \cdots & \cdots \\ b_{1n} & \cdots & b_{nn} \end{vmatrix} ,$$

in other words, every basis-element of $\mathfrak{R}'(\mathfrak{a})$ is b-times the corresponding basis-element of $\mathfrak{R}(\mathfrak{a})$. Hence we find

Theorem 3. The ideal $\dfrac{\mathfrak{R}(\mathfrak{a})}{\mathfrak{R}(\mathfrak{o})}$ *does not depend on the field-basis* ω_i, *but only on the ideal* $\mathfrak{a}$.

Indeed, it follows from the above that

$$\frac{\mathfrak{R}'(\mathfrak{a})}{\mathfrak{R}'(\mathfrak{o})} = \frac{\mathfrak{R}(\mathfrak{a}) \cdot b}{\mathfrak{R}(\mathfrak{o}) \cdot b} = \frac{\mathfrak{R}(\mathfrak{a})}{\mathfrak{R}(\mathfrak{o})} \;,$$

b differing from 0.

In particular, if ω'_j is a permutation of ω_i, then the determinant b is equal either to 1 or to -1; both cases determine entirely the same array-ideals, i. e., $\mathfrak{R}(\mathfrak{a})$ is independent of the order of the basis-elements of the field P.

It should be observed that $\dfrac{\mathfrak{R}(\mathfrak{a})}{\mathfrak{R}(\mathfrak{o})}$ is already an integral ideal. This is an obvious consequence of the congruence (1).

The ideal $\dfrac{\mathfrak{R}(\mathfrak{a})}{\mathfrak{R}(\mathfrak{o})}$ depending only on the ideal $\mathfrak{a}$ but neither on the basis of $\mathfrak{a}$ nor on that of the field P will be denoted by $\mathfrak{M}(\mathfrak{a})$.

In order to deduce another representation of $\mathfrak{M}(\mathfrak{a})$, let us consider the array-ideal

$$\mathfrak{a}^* = \left(\left(\begin{matrix} \alpha_1^{(1)} & \dots & \alpha_1^{(n)} \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \alpha_M^{(1)} & \dots & \alpha_M^{(n)} \end{matrix}\right)\right).$$

This is an ideal in a Galois-over-field of Ω containing P. A basis-element of $\mathfrak{a}^*$ is

$$\begin{vmatrix} \alpha_{\mu_1}^{(1)} & \dots & \alpha_{\mu_1}^{(n)} \\ \dots & \dots & \dots \\ \alpha_{\mu_n}^{(1)} & \dots & \alpha_{\mu_n}^{(n)} \end{vmatrix} = \begin{vmatrix} \sum_{i=1}^{n} r_{\mu_1 i}\,\omega_i^{(1)} & \dots & \sum_{i=1}^{n} r_{\mu_1 i}\,\omega_i^{(n)} \\ \dots & \dots & \dots \\ \sum_{i=1}^{n} r_{\mu_n i}\,\omega_i^{(1)} & \dots & \sum_{i=1}^{n} r_{\mu_n i}\,\omega_i^{(n)} \end{vmatrix} =$$

$$= \begin{vmatrix} r_{\mu_1 1} & \dots & r_{\mu_n 1} \\ \dots & \dots & \dots \\ r_{\mu_1 n} & \dots & r_{\mu_n n} \end{vmatrix} \cdot \begin{vmatrix} \omega_1^{(1)} & \dots & \omega_n^{(1)} \\ \dots & \dots & \dots \\ \omega_1^{(n)} & \dots & \omega_n^{(n)} \end{vmatrix},$$

where the determinant

$$\begin{vmatrix} \omega_1^{(1)} & \dots & \omega_n^{(1)} \\ \dots & \dots & \dots \\ \omega_1^{(n)} & \dots & \omega_n^{(n)} \end{vmatrix}$$

is different from 0 because of $\omega_1, \dots, \omega_n$ being linearly independent. Hence we infer that

$$\mathfrak{a}^* = \mathfrak{N}(\mathfrak{a}) \cdot \begin{vmatrix} \omega_1^{(1)} & \dots & \omega_n^{(1)} \\ \dots & \dots & \dots \\ \omega_1^{(n)} & \dots & \omega_n^{(n)} \end{vmatrix},$$

and similarly the array-ideal [15])

$$\mathfrak{o}^* = \left(\left(\begin{matrix} o_1^{(1)} & \dots & o_1^{(n)} \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ o_N^{(1)} & \dots & o_N^{(n)} \end{matrix}\right)\right)$$

is equal to

$$\mathfrak{N}(\mathfrak{o}) \cdot \begin{vmatrix} \omega_1^{(1)} & \dots & \omega_n^{(1)} \\ \dots & \dots & \dots \\ \omega_1^{(n)} & \dots & \omega_n^{(n)} \end{vmatrix}.$$

[15]) We make a point of the interesting fact that the square of $\mathfrak{o}^*$ is already an ideal of Σ and in the case of algebraic numbers it is just equal to the relative discriminant of P with respect to Ω (cf. footnote[2])). For the definition of the relative discriminant see *Hilbert* [1], § 14.

In connection with the preceding theorem, we are led to formulate the following theorem.

Theorem 4. The ideal $\mathfrak{M}(\mathfrak{a}) = \dfrac{\mathfrak{a}^*}{\mathfrak{d}^*}$ *being the quotient of two array-ideals depends only on the ideal* $\mathfrak{a}$.

Next we pass to the proof of

Theorem 5[16]). *The norm of* $\mathfrak{a}$ in Γ *is equal to that of* $\mathfrak{M}(\mathfrak{a})$ *in* Σ:

$$n(\mathfrak{a}) = N(\mathfrak{M}(\mathfrak{a})) \ .$$

Consider the set of the elements of the residue-class-ring $\Sigma/\mathfrak{R}_l(\mathfrak{a})$; this can be regarded as a set of elements of Σ, no two of which are congruent mod $\mathfrak{R}_l(\mathfrak{a})$, but every element of Σ is congruent with one of them mod $\mathfrak{R}_l(\mathfrak{a})$. [We remember that it was assumed that in $\Sigma/\mathfrak{R}_l(\mathfrak{a})$ there exist elements only in a finite number.]

Let $s_l \in \Sigma$ denote the elements of the residue-class-ring $\Sigma/\mathfrak{R}_l(\mathfrak{a})$, which are $\equiv 0\,(\mathfrak{R}_l(\mathfrak{o}))$. An element

$$\sigma_l = \sum_{\kappa=1}^{l} s_{l\kappa}\,\omega_\kappa \qquad (s_{l\kappa}\,\varepsilon\,\Omega)$$

of Γ may be taken to be subjected to the postulate $s_{ll} = s_l$. Take further to every s_l one σ_l of this type and fix them. If

$$\beta = \sum_{l=1}^{n} \sigma_l \quad \text{and} \quad \beta' = \sum_{l=1}^{n} \sigma_l'$$

are two elements of Γ, then from the congruence

$$\beta \equiv \beta'\,(\mathfrak{a}) \ ,$$

i. e.,

$$\beta - \beta' = \sum_{l=1}^{n} (\sigma_l - \sigma_l') = \sum_{\kappa=1}^{n-1} t_\kappa\,\omega_\kappa + (s_n - s_n')\,\omega_n \equiv 0\,(\mathfrak{a})$$

it is not difficult to conclude that $s_n = s_n'$; indeed, by definition

$$s_n \equiv s_n'\,(\mathfrak{R}_n(\mathfrak{a})) \ ,$$

and s_n and s_n' are elements of the residue-class-ring $\Sigma/\mathfrak{R}_n(\mathfrak{a})$. Thus for the corresponding σ_n and σ_n' also equality holds: $\sigma_n = \sigma_n'$. Proceeding

---

[16]) The ideal-norm will be denoted in Σ by N and in Γ by n.

in this way, we obtain successively $\sigma_{n-1} = \sigma'_{n-1}, \ldots,$ finally we arrive at $\sigma_1 = \sigma'_1$. Therefore $\beta = \beta'$. This means, no two different of the elements of the form $\sum_{l=1}^{n} \sigma_l$ are congruent mod $\mathfrak{a}$.

On the other hand, if $\eta = \sum_{l=1}^{n} b_l \omega_l$ is an element of Γ, then $b_n \equiv 0\,(\mathfrak{R}_n(\mathfrak{o}))$ involves that b_n is congruent with an s_n mod $\mathfrak{R}_n(\mathfrak{a})$, say,

$$b_n \equiv s_n^* \,(\mathfrak{R}_n(\mathfrak{a}))\,,$$

and so evidently for σ_n^* corresponding to s_n^* we get

$$\eta - \sigma_n^* \equiv \sum_{k=1}^{n-1} b'_k \,\omega_k(\mathfrak{a}) \,.$$

Similarly, putting $b'_{n-1} \equiv s_{n-1}^* (\mathfrak{R}_{n-1}(\mathfrak{a}))$ we have

$$\eta - \sigma_{n-1}^* - \sigma_n^* \equiv \sum_{\kappa=1}^{n-2} b''_\kappa \,\omega_\kappa(\mathfrak{a})$$

and likewise let us continue until this process comes to an end. As result

$$\eta \equiv \sum_{l=1}^{n} \sigma_l^* \,(\mathfrak{a})$$

is obtained, which establishes that each element of Γ is congruent with one and only one of the elements of the type $\sum_{l=1}^{n} \sigma_l$. The finite number of the different s_l is evidently

$$\frac{N(\mathfrak{R}_l(\mathfrak{a}))}{N(\mathfrak{R}_l(\mathfrak{o}))} = N\left(\frac{\mathfrak{R}_l(\mathfrak{a})}{\mathfrak{R}_l(\mathfrak{o})}\right),$$

thus the norm of $\mathfrak{a}$ is equal to the product of $N\left(\frac{\mathfrak{R}_l(\mathfrak{a})}{\mathfrak{R}_l(\mathfrak{o})}\right)$. This leads us to the result

$$n(\mathfrak{a}) = \prod_{l=1}^{n} N\left(\frac{\mathfrak{R}_l(\mathfrak{a})}{\mathfrak{R}_l(\mathfrak{o})}\right) = N\left(\frac{\mathfrak{R}_1(\mathfrak{a})\ldots\mathfrak{R}_n(\mathfrak{a})}{\mathfrak{R}_1(\mathfrak{o})\ldots\mathfrak{R}_n(\mathfrak{o})}\right) = N\left(\frac{\mathfrak{R}(\mathfrak{a})}{\mathfrak{R}(\mathfrak{o})}\right),$$

that is to say,

$$n(\mathfrak{a}) = N(\mathfrak{M}(\mathfrak{a}))\,, \qquad \text{q. e. d}^{17)}.$$

---

17) The proved theorem also involves that the residue-class-ring $\Gamma/\mathfrak{a}$ contains but a finite number of elements.

Since the same relation

$$n(\mathfrak{a}) = N(\mathfrak{N}(\mathfrak{a}))$$

is true also for the Hilbertian relative norm of $\mathfrak{a}$ defined as the product of its conjugates

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{a}^{(1)} \dots \mathfrak{a}^{(n)} ,$$

we have got the relation

$$N(\mathfrak{M}(\mathfrak{a})) = N(\mathfrak{N}(\mathfrak{a})) .$$

In order to prove the equality of $\mathfrak{M}(\mathfrak{a})$ and $\mathfrak{N}(\mathfrak{a})$, let us take such elements α_1 and α_2 in $\mathfrak{a}$ that their norms[18])

$$\mathfrak{n}(\alpha_1) = \alpha_1^{(1)} \dots \alpha_1^{(n)} \qquad \text{and} \qquad \mathfrak{n}(\alpha_2) = \alpha_2^{(1)} \dots \alpha_2^{(n)}$$

could be considered as a basis of the relative norm $\mathfrak{N}(\mathfrak{a})$:

$$\mathfrak{N}(\mathfrak{a}) = (\mathfrak{n}(\alpha_1), \mathfrak{n}(\alpha_2)) .$$

The ideal $\mathfrak{a}^*$ contains both the array-ideal[19])

$$\left(\begin{pmatrix} \alpha_1^{(1)} o_1^{(1)} \dots \alpha_1^{(n)} o_1^{(n)} \\ \dots\dots\dots\dots\dots \\ \dots\dots\dots\dots\dots \\ \alpha_1^{(1)} o_N^{(1)} \dots \alpha_1^{(n)} o_N^{(n)} \end{pmatrix}\right) = \alpha_1^{(1)} \dots \alpha_1^{(n)} \cdot \mathfrak{o}^* = \mathfrak{n}(\alpha_1) \cdot \mathfrak{o}^*$$

---

18) There is no difficulty in extending the proof of the corresponding theorem on absolute norm given in *Hilbert* [1] (theorem 21) to our case: be $a_1 \varepsilon\, \mathfrak{N}(\mathfrak{a})$ and choose a_2 so that

$$\left(a_1, \frac{a_2}{\mathfrak{a}}\right) = \mathfrak{o}$$

then also

$$\left(a_1, \frac{\mathfrak{n}(a_2)}{\mathfrak{N}(\mathfrak{a})}\right) = \mathfrak{o} .$$

Hence

$$(a_1^n, \mathfrak{n}(a_2)) = \mathfrak{N}(\mathfrak{a}),$$

i. e.

$$(\mathfrak{n}(a_1), \mathfrak{n}(a_2)) = \mathfrak{N}(\mathfrak{a})$$

is implied.

19) If a is an element of $\mathfrak{a}$, then all of $a\, o_1, \dots, a\, o_N$ are in $\mathfrak{a}$, hence $(a_1, \dots, a_M, a o_1, \dots a\, o_N)$ is a basis of $\mathfrak{a}$, provided $(a_1, \dots, a_M)$ is a basis too. Therefore, the array-ideal $\bar{\mathfrak{a}}^*$ made up of the conjugates of $a_1, \dots, a_M, a\, o_1, \dots, a\, o_N$ is equal to $\mathfrak{a}^*$. Among the basis-elements of $\bar{\mathfrak{a}}^*$, however, the basis-elements of $\left((a^{(i)} o_\nu^{(i)})\right)$ occur; this means, $\left((a^{(i)} o_\nu^{(i)})\right)$ is contained in $\mathfrak{a}^*$, indeed.

and the array-ideal

$$\left(\left(\begin{matrix} \alpha_2^{(1)} o_1^{(1)} \ldots \alpha_2^{(n)} o_1^{(n)} \\ \ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots \\ \alpha_2^{(1)} o_N^{(1)} \ldots \alpha_2^{(n)} o_N^{(n)} \end{matrix}\right)\right) = \alpha_2^{(1)} \ldots \alpha_2^{(n)} \cdot \mathfrak{o}^* = \mathfrak{n}(\alpha_2) \cdot \mathfrak{o}^* \ .$$

Therefore $\mathfrak{N}(\mathfrak{a}) = (\mathfrak{n}(\alpha_1), \mathfrak{n}(\alpha_2))$ is a multiple of $\mathfrak{M}(\mathfrak{a}) = \dfrac{\mathfrak{a}^*}{\mathfrak{o}^*}$,

$$\mathfrak{N}(\mathfrak{a}) \equiv 0 \ (\mathfrak{M}(\mathfrak{a})) \ .$$

Now remember that $\mathfrak{M}(\mathfrak{a})$ and $\mathfrak{N}(\mathfrak{a})$ have the same norm, so the equality of $\mathfrak{M}(\mathfrak{a})$ and $\mathfrak{N}(\mathfrak{a})$ is necessarily implied:

$$\mathfrak{M}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a}) \ .$$

To sum up our results, we have proved:

Theorem 6. The relative norm of an ideal $\mathfrak{a}$ *is the quotient of the array-ideals* $\mathfrak{a}^* = ((\alpha_\mu^{(i)}))$ *and* $\mathfrak{o}^* = ((o_\nu^{(i)}))$:

$$\mathfrak{N}(\mathfrak{a}) = \frac{\mathfrak{a}^*}{\mathfrak{o}^*} \ .$$

(Eingegangen den 10. Februar 1947.)

INDEX OF WORKS REFERRED TO

R. Dedekind [1]: Vorlesungen über Zahlentheorie, Suppl. XI, Braunschweig 1894.

E. Hecke [1]: Theorie der algebraischen Zahlen, Leipzig 1923.

D. Hilbert [1]: Bericht über die Theorie der algebraischen Zahlen, Jahresbericht der Deutschen Math. Ver., vol. 4, 1897.

E. Landau [1]: Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale, Leipzig 1918.

[2]: Vorlesungen über Zahlentheorie, vol. III, Leipzig 1927.

E. Noether [1]: Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern, Math. Annalen 96 (1927), pp. 21—61.

B. L. van der Waerden [1]: Moderne Algebra, vol. I, Berlin 1937.

[2]: Moderne Algebra, vol. II, Berlin 1940.