SOME THEOREMS ON ALGEBRAIC RINGS.

By

LADISLAS FUCHS

in BUDAPEST.

In his paper "Sätze über algebraische Ringe"[1] T. Nagell has discussed certain properties of algebraic rings. The present note concerns itself with the generalization of these results to relative algebraic rings; the theorems will be transferred without essential change.

In what follows we shall mean by F a finite algebraic number field and by R the ring of the integral elements of F. Let further ϕ be an algebraic field over F of degree n and let P be the ring of the integral elements of ϕ. It is well known that in ϕ there are n elements[2], $\omega_1, \ldots, \omega_n$, being linearly independent with respect to F, such that every element of ϕ possesses a unique representation of the form

$$\omega = a_1 \omega_1 + \cdots + a_n \omega_n \tag{1}$$

with coefficients in F. The ω_i are called the basis of ϕ with respect to F. Let ξ be an element of P of the exact degree n, that is, ξ is a root of an *irreducible* algebraic equation $x^n + r_1 x^{n-1} + \cdots + r_n = 0$ where r_i are in R. In view of (1) we may set

$$\xi^k = c_{k1} \omega_1 + \cdots + c_{kn} \omega_n, \qquad (c_{ki} \varepsilon F) \tag{2}$$

for $k = 0, 1, \ldots, n-1$. Since ξ was chosen so as to be of the exact degree n, the determinant $c = |c_{ki}|$ of the coefficients in (2) does not vanish, and so the system may be inverted, and then we get

$$\omega_i = \frac{1}{c}(b_{i1} + b_{i2}\xi + \cdots + b_{in}\xi^{n-1}), \qquad (b_{ik} \varepsilon F) \tag{3}$$

for $i = 1, 2, \ldots, n$.

---

[1] Math. Zeitschrift 34 (1932), pp. 179—182.

[2] The elements of F will be denoted by Latin, those of ϕ by Greek letters.

For the sake of convenience we suppose that the ω_i were so chosen that whenever ω in (1) is integer, the a_i are all integers, i. e., are all in R. Then so are of course the c_{ki} in (2) [and hence c] as well as the b_{ik} in (3).

On account of (1) and (3) one sees at once that

$$\omega = \frac{1}{c} \sum_{i=1}^{n} a_i (b_{i1} + b_{i2}\xi + \cdots + b_{in}\xi^{n-1}) = \frac{1}{c} \{ (\Sigma a_i b_{i1}) + \cdots + (\Sigma a_i b_{in}) \xi^{n-1} \},$$

that is to say, by means of the powers of ξ every element of P has a representation of the form

$$\omega = \frac{1}{c}(c_1 + c_2 \xi + \cdots + c_n \xi^{n-1}), \qquad (c_i \varepsilon R). \tag{4}$$

(4) is unique in c_i, for $1, \xi, \ldots, \xi^{n-1}$ are linearly independent with respect to R.

Let now P^* be a subring of P containing ξ. Every element γ of P^* may clearly be represented in the form

$$\gamma = \frac{1}{c}(c_1 + c_2 \xi + \cdots + c_l \xi^{l-1}), \qquad (c_i \varepsilon R,\ 1 \leq l \leq n)$$

where $c_l \neq 0$. Consider all the γ for a fixed number l. It is easily seen that the last coefficients[3] c_l constitute an ideal in R. That this ideal $\mathfrak{L}_l$ must contain a non-vanishing element and so $\mathfrak{L}_l$ is distinct from the zero-ideal, is evident. Setting $\mathfrak{L}_l = (c_l^{(1)}, \ldots, c_l^{(m_l)})$, it is also evident that to each basis element $c_l^{(\mu)}$ there corresponds a number $\gamma_l^{(\mu)}$ of P^* with the last coefficient $c_l^{(\mu)}$:

$$\begin{gathered} \gamma_l^{(\mu)} = \frac{1}{c}(c_{l1}^{(\mu)} + c_{l2}^{(\mu)} \xi + \cdots + c_{ll}^{(\mu)} \xi^{l-1}) \\ (c_{lj}^{(\mu)} \varepsilon R, \quad c_{ll}^{(\mu)} = c_l^{(\mu)}, \quad \mu = 1, \ldots, m_l). \end{gathered} \tag{5}$$

The elements $\gamma_1^{(1)}, \ldots, \gamma_1^{(m_1)}, \gamma_2^{(1)}, \ldots, \gamma_2^{(m_2)}, \ldots, \gamma_n^{(1)}, \ldots, \gamma_n^{(m_n)}$, or, if we want to have the indices running successively from 1 until $N = \sum_{l=1}^{n} m_l$, the elements $\gamma_1, \ldots, \gamma_N$ form a basis of P^* with respect to R, that is to say, *every element of P^* can be expressed in the form*

$$\gamma = d_1 \gamma_1 + \cdots + d_N \gamma_N, \qquad (d_\nu \varepsilon R). \tag{6}$$

However, this representation is not unique, in general.

---

[3] More precisely: the c-times of the last coefficients.

The powers of ξ are in P^*, we can therefore find numbers x of R such that for $k > 1$

$$\xi^{k-1} = \sum_{l=1}^{k} (x_l^{(1)} \gamma_l^{(1)} + \cdots + x_l^{(m_l)} \gamma_l^{(m_l)}), \qquad (x_l^{(\mu)} \varepsilon R). \tag{7}$$

If we replace here $\gamma_l^{(\mu)}$ by their values taken from (5), one sees immediately that the coefficient of ξ^{k-1} is 1 on the left side, while on the right side

$$\frac{1}{c}(x_k^{(1)} c_k^{(1)} + \cdots + x_k^{(m_k)} c_k^{(m_k)}) = \frac{c_k}{c}$$

c_k being a number of $\mathfrak{L}_k$. From the equality of the two coefficients, implied by the linear independence of $1, \xi, \ldots, \xi^{k-1}$, it follows $c = c_k$. We thus get that c is an element of every $\mathfrak{L}_k (k > 1)$:

Theorem 1. *The determinant* $c = |c_{ki}|$ *is divisible by* $\mathfrak{L}_k$ *for* $k > 1$.

We further get from (5) the equality

$$\gamma_l^{(\mu)} \cdot \xi^{j-l} = \frac{1}{c}(c_{l1}^{(\mu)} \xi^{j-l} + \cdots + c_{ll}^{(\mu)} \xi^{j-1})$$

showing that $c_{ll}^{(\mu)}$ and similarly, every basis element of $\mathfrak{L}_l$ is contained in $\mathfrak{L}_j$ for $l \leq j$. This implies that $\mathfrak{L}_l \equiv 0 (\mathfrak{L}_j)$ for $l \leq j$, that is in words,

Theorem 2. $\mathfrak{L}_l$ *is divisible by* $\mathfrak{L}_j$ *if* $l \leq j$.

Let us now turn our attention to the proof of

Theorem 3. $c_{lj}^{(\mu)}$ *is divisible by* $\mathfrak{L}_l$.

Proof by the principle of mathematical induction. For $l = 1$ the assertion is trivial. Let us suppose that $c_{kj}^{(\mu)}$ for $k \leq l - 1$ is divisible by $\mathfrak{L}_k$ and so a fortiori by $\mathfrak{L}_{l-1}$, in accordance with theorem 2. Consider $\gamma_l^{(\mu)}$ and take an element c' of $\frac{\mathfrak{L}_{l-1}}{\mathfrak{L}_l}$. The last coefficient[3] of $c' \gamma_l^{(\mu)}$, $c' c_l^{(\mu)}$ lies in $\mathfrak{L}_{l-1}$, therefore elements $y_i \varepsilon R$ can always be chosen such that $c' c_l^{(\mu)} = y_1 c_{l-1}^{(1)} + \cdots + y_{m_{l-1}} c_{l-1}^{(m_{l-1})}$ holds. Hence we conclude that $c' \gamma_l^{(\mu)} - (y_1 \gamma_{l-1}^{(1)} + \cdots + y_{m_{l-1}} \gamma_{l-1}^{(m_{l-1})}) \xi$ contains only powers of ξ with exponents not greater than $l - 2$; so that we obtain

$$c' \gamma_l^{(\mu)} = \sum_{k=1}^{l-1} (x_k^{(1)} \gamma_k^{(1)} + \cdots + x_k^{(m_k)} \gamma_k^{(m_k)}) + (y_1 \gamma_{l-1}^{(1)} \xi + \cdots + y_{m_{l-1}} \gamma_{l-1}^{(m_{l-1})} \xi).$$

Setting here for the $\gamma_k^{(\varrho)}$ their values taken from (5), we see that on the right hand side the first subscripts of $c_{kj}^{(\varrho)}$ are not greater than $l - 1$, therefore by assumption we may hence conclude that the (c-times) coefficients of the powers of ξ are divisible by $\mathfrak{L}_{l-1}$. The fact that the coefficients of the same powers of ξ must be equal on the two sides implies that $c' c_{ij}^{(\mu)} \equiv 0 (\mathfrak{L}_{l-1})$. Since c' was arbitrary in $\frac{\mathfrak{L}_{l-1}}{\mathfrak{L}_l}$, we finally get that $c_{ij}^{(\mu)}$ must be contained in $\mathfrak{L}_l$, and this completely establishes the theorem.

We now pass to the proof of the following theorem.

Theorem 4. *The relative discriminant of P^* with respect to R:*

$$\vartheta_{P^*/R} = \frac{1}{c^{2n}} (\mathfrak{L}_1 \ldots \mathfrak{L}_n)^2 \cdot D(\xi) \tag{8}$$

where $D(\xi)$ is the relative discriminant of ξ.

All the determinants of order n of the matrix[4]

$$\begin{pmatrix} \gamma_1^{(1)} \gamma_2^{(1)} \ldots \gamma_N^{(1)} \\ \gamma_1^{(2)} \gamma_2^{(2)} \ldots \gamma_N^{(2)} \\ \cdots\cdots\cdots \\ \gamma_1^{(n)} \gamma_2^{(n)} \ldots \gamma_N^{(n)} \end{pmatrix}$$

generate an ideal $\mathfrak{L}^*$ in a Galois-overfield of F containing ϕ. The square of $\mathfrak{L}^*$ is an ideal in R and is equal to the relative discriminant of P^* with respect to R. $\mathfrak{L}^*$ may easily be verified to be the $\frac{1}{c^n}$-times product of

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \xi^{(1)} & \xi^{(2)} & \ldots & \xi^{(n)} \\ \cdots & \cdots & \cdots & \cdots \\ \xi^{(1)^{n-1}} & \xi^{(2)^{n-1}} & \ldots & \xi^{(n)^{n-1}} \end{vmatrix}$$

and the ideal $\mathfrak{L}$ generated by the n-ordered determinants of

$$\begin{pmatrix} c_{11}\, c_{21} \ldots c_{N1} \\ c_{12}\, c_{22} \ldots c_{N2} \\ \cdots\cdots\cdots \\ c_{1n}\, c_{2n} \ldots c_{Nn} \end{pmatrix}$$

[4] $\gamma_\nu^{(i)}$ is the ith conjugate of γ_ν.

where the $c_{\nu i}$ are the coefficients for which

$$\gamma_\nu = \frac{1}{c}\left(\sum_{i=1}^{n} c_{\nu i}\, \xi^{i-1}\right)$$

(cf. (5); some of $c_{\nu i}$ are vanishing). As I have proved elsewhere[5], $\mathfrak{L}$ is equal to the idealproduct $\mathfrak{L}_1 \ldots \mathfrak{L}_n$, so that we are led to the result enunciated in theorem 4.

[5] A theorem on the relative norm of an ideal, Commentarii Math. Helvetici 21 (1948), pp. 29—43; see theorem 1.