ON THE BASE OF A RELATIVE NUMBER-FIELD, WITH AN APPLICATION TO THE COMPOSITION OF FIELDS*

BY

G. E. WAHLIN

It is a well known fact that in an algebraic number-field of degree n there exist n integers $\alpha_1, \cdots, \alpha_n$ such that every integer of the field can be expressed in the form

$$\omega = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n,$$

where $x_1, x_2, x_3, \cdots, x_n$ are rational integers.

If we now consider a field relative to a given subfield of this field, from the nature of the proof of the above fact it is evident that, if the subfield in question is such that the number of classes of ideals in this field is one, and r the degree of the larger field relative to its subfield, then there exist r integers $\beta_1, \beta_2, \cdots, \beta_r$ such that every integer in the larger field can be expressed in the form

$$\omega = y_1\beta_1 + y_2\beta_2 + \cdots + y_r\beta_r,$$

where now $y_1, y_2, \cdots, y_r$ are integers in the subfield.

When, however, the number of classes of the subfield is greater than one, this is not the case. SOMMER† has shown that in this case for a field which is of the second degree relative to a subfield of the second degree the four numbers composing the base may be taken to be $\omega_1, \omega_2, \beta_1\Omega, \beta_2\Omega$, where ω_1, ω_2 is the base of the subfield and β_1, β_2 the base of an ideal in the subfield and Ω a number of the larger field, not necessarily an integer, but such that $\beta_1\Omega$ and $\beta_2\Omega$ are integers in this field.

In the first part of this paper I establish a similar form for the base of any algebraic number-field relative to any subfield, and in the last part I apply this to the study of the discriminant of the field.

The Base of a Relative Field.

Let K be an algebraic number-field of degree N which contains the subfield k of degree n. We then know that $r = N/n$ is the degree of K relative to k, and if ϑ be any integer which determines the field K, then ϑ is the root of an

* Presented to the Society (Chicago), December 31, 1909.

† SOMMER, *Vorlesungen über Zahlentheorie*, p. 299.

equation

$$x^r + \alpha_1 x^{r-1} + \alpha_2 x^{r-2} + \cdots + \alpha_r = 0, \tag{1}$$

where $\alpha_1, \alpha_2, \cdots, \alpha_r$ are integers in k. We therefore know that every number of K can be expressed in the form

$$\omega = \rho_1 + \rho_2 \vartheta + \rho_3 \vartheta^2 + \cdots + \rho_r \vartheta^{r-1}, \tag{2}$$

where $\rho_1, \rho_2, \cdots, \rho_r$ are numbers of the subfield k. Then, in the same manner as when we consider a field relative to the domain of rational integers, we can show that every integer in K can be expressed in the form

$$\omega = \frac{A_1 + A_2 \vartheta + A_3 \vartheta^2 + \cdots + A_r \vartheta^{r-1}}{D_k(\vartheta)}, \tag{3}$$

where $A_1, A_2, \cdots, A_r$ are integers in k and $D_k(\vartheta)$ is the relative discriminant of ϑ with respect to k.*

Let us now consider all integers of K for which $A_{\tau+1} = A_{\tau+2} = \cdots = A_r = 0$, where τ is one of the integers $1, 2, 3, \cdots, r$. These integers we can indicate as follows

$$\omega_\tau^{(i)} = \frac{O_{1\tau}^{(i)} + O_{2\tau}^{(i)} \vartheta + O_{3\tau}^{(i)} \vartheta^2 + \cdots + O_{\tau\tau}^{(i)} \vartheta^{\tau-1}}{D_k(\vartheta)} \quad (i = 1, 2, 3, \cdots). \tag{4}$$

It is evident that any integer of the type (4) when multiplied by an integer of k gives another integer of the same type, and the sum of any number of such integers is also an integer of this type. But this means that the product of any one of the coefficients $O_{\tau\tau}^{(i)}$ by an integer of k gives another of these integers and, moreover, the sum of any number of them is also another integer of the same set. Hence, since all the integers $O_{\tau\tau}^{(i)}$ belong to k, they form an ideal in this field, which ideal is the highest common ideal factor of all these coefficients. This ideal we shall designate by O_τ.

Thus, for $\tau = 1, 2, 3, \cdots, r$ we get r ideals $O_1, O_2, O_3, \cdots, O_r$ in k. But since $\omega_1^{(i)} = O_{11}^{(i)}/D_k(\vartheta)$ is a number of k and, moreover, from our assumption an integer, and since evidently all integers of k are thus represented, k being a subfield of K, and r being the lowest degree of the equation which ϑ satisfies in k, we conclude that $O_{11}^{(i)}$ $(i = 1, 2, 3, \cdots)$ represent all multiples $D_k(\vartheta)$ in k and therefore the ideal O_1 is the principal ideal $[D_k(\vartheta)]$. Moreover, since $\vartheta \cdot \omega_{\tau-1}^{(i)}$ evidently is an integer of K of the type (4), we conclude that all the integers of $O_{\tau-1}$ also belong to O_τ, and hence that $O_{\tau-1}$ is divisible by O_τ. Therefore, in the sequence $O_1, O_2, O_3, \cdots, O_r$ each ideal is a factor of all that precede it in the sequence, and hence all of them are factors of $D_k(\vartheta)$. Therefore, the integer $D_k(\vartheta)$ belongs to each one of these ideals. But we know that if we choose arbitrarily from an ideal any integer

* HILBERT, Jahresbericht der deutschen Mathematiker-Vereinigung, vol. 4 (1894–95), p. 180.

there exists another integer such that the given ideal is the greatest common divisor of these two integers. Hence each of the above ideals must contain an integer such that the ideal in question is the greatest common divisor of this integer and $D_k(\vartheta)$. If we then let this integer in O_τ be the coefficient $O^{(1)}_{\tau\tau}$ we can write

$$O_\tau = [O^{(1)}_{\tau\tau},\ D_k(\vartheta)] \qquad (\tau = 1, 2, 3, \cdots, r).$$

Let us now put $D_k(\vartheta)/O_\tau = I_\tau$. Evidently I_τ is relatively prime to $O^{(1)}_{\tau\tau}$ and, hence, there exists in k an integer β such that

$$O^{(1)}_{\tau\tau}\cdot\beta \equiv 1 \qquad (I_\tau).$$

Hence, if we indicate by $\bar{\omega}_\tau$ the numerator in the expression for $\omega^{(1)}_\tau$, we have the following congruence

$$\bar{\omega}_\tau\cdot\beta = (O^{(1)}_{1\tau} + O^{(1)}_{2\tau}\vartheta + O^{(1)}_{3\tau}\vartheta^2 + \cdots + O^{(1)}_{\tau\tau}\vartheta^{\tau-1})\cdot\beta \equiv \bar{\Omega}_\tau \qquad (I_\tau),$$

where

$$\bar{\Omega}_\tau = A_{1\tau} + A_{2\tau}\vartheta + A_{3\tau}\vartheta^2 + \cdots + A_{\tau-1\tau}\vartheta^{\tau-2} + \vartheta^{\tau-1}.$$

We observe that in $\bar{\Omega}_\tau$ the coefficient of $\vartheta^{\tau-1}$ is unity. But since $\omega^{(1)}_\tau = \bar{\omega}_\tau/D_k(\vartheta)$ is an integer, it follows that $\bar{\omega}_\tau$ is divisible by $D_k(\vartheta)$ and hence by I_τ. From the last congruence it follows that also $\bar{\Omega}_\tau$ is divisible by I_τ.

The quotient $\Omega_\tau = \bar{\Omega}_\tau/D_k(\vartheta)$ is not necessarily an integer in K, but $D_k(\vartheta)\cdot\Omega_\tau$ and $O^{(1)}_{\tau\tau}\Omega_\tau$ are evidently both integers in K.

Let

$$\omega = \frac{\beta_1 + \beta_2\vartheta + \beta_3\vartheta^2 + \cdots + \beta_r\vartheta^{r-1}}{D_k(\vartheta)} \tag{5}$$

be any integer in K. From what we have seen above β_r belongs to the ideal $O_r = [O^{(1)}_{rr},\ D_k(\vartheta)]$ and, hence, there exist in k two integers λ_r and μ_r such that

$$\lambda_r O^{(1)}_{rr} + \mu_r D_k(\vartheta) = \beta_r. \tag{6}$$

But then

$$\beta_r\Omega_r = \lambda_r O^{(1)}_{rr}\Omega_r + \mu_r D_k(\vartheta)\cdot\Omega_r,$$

which is evidently an integer in K and, moreover, this integer when expressed in the form (4) has the same coefficient of ϑ^{r-1} as ω in (5). Hence $\omega - \beta_r\Omega_r$ is an integer of the type

$$\frac{\beta'_1 + \beta'_2\vartheta + \beta'_3\vartheta^2 + \cdots \beta'_{r-1}\vartheta^{r-2}}{D_k(\vartheta)}.$$

In the same manner as above we can determine λ_{r-1} and μ_{r-1} such that

$$\beta'_{r-1} = \lambda_{r-1}O^{(1)}_{r-1\,r-1} + \mu_r D_k(\vartheta), \tag{6^a}$$

and $\beta'_{r-1}\Omega_{r-1}$ is then an integer of K of the type (4) when $\tau = r-1$ and the coefficient of ϑ^{r-2} is β'_{r-1}.

Hence we have

$$\omega - \beta_r \Omega_r - \beta'_{r-1}\Omega_{r-1} = \frac{\beta''_1 + \beta''_2 \vartheta + \cdots + \beta''_{r-2}\vartheta^{r-3}}{D_k(\vartheta)},$$

which is again an integer.

By continuing in this manner we evidently shall at last have

$$\omega - \beta_r \Omega_r - \beta'_{r-2}\Omega_{r-1} - \cdots - \beta_1^{(r-1)}\Omega_1 = 0,$$

whence

$$\omega = \beta_1^{(r-1)}\Omega_1 + \beta_2^{(r-2)}\Omega_2 + \cdots + \beta_r \Omega_r, \tag{7}$$

where, for all values of s from 1 to r, $\beta_s^{(r-s)}$ is an integer belonging to the ideal O_s. Now ω is any integer of K and, hence, every integer of K can be represented in the form (7). Moreover, since $O_{\tau\tau}^{(1)}\Omega_\tau$ and $D_k(\vartheta)\Omega_\tau$ are both integers in K, from (6) and (6^a) and the similar expressions for the remaining $\beta_s^{(r-s)}$ we can conclude that when $\beta_s^{(r-s)}$ belongs to the ideal O_s all numbers represented by (7) are integers of the field K.

If we now let $(i_{1\tau}, i_{2\tau}, \cdots, i_{n\tau})$ be the base of the ideal O_τ, then evidently the N integers $i_{\lambda\tau}\Omega_\tau (\lambda = 1, 2, 3 \cdots n;\ \tau = 1, 2, 3 \cdots r)$ form a base of all the integers in the field K. By replacing in this base $\Omega_1, \Omega_2, \Omega_3, \cdots, \Omega_r$ by their relative conjugates with respect to the field k we get the basis of the respective relative conjugate fields.

The Relative Discriminant of K.

Let us now apply this result to the relative discriminant of the field K with respect to k. The relative discriminant is defined as the greatest common factor of the squares of all the determinants formed from the matrix of the base of K and its relative conjugates. It is easily seen that each of the determinants can be written

$$i_{\lambda_1\tau_1} \cdot i_{\lambda_2\tau_2} \cdots i_{\lambda_r\tau_r} \begin{vmatrix} \Omega_{\tau_1}, & \Omega_{\tau_2}, & \cdots, & \Omega_{\tau_r} \\ \Omega_{\tau_1}^{(1)}, & \Omega_{\tau_2}^{(1)}, & \cdots, & \Omega_{\tau_r}^{(1)} \\ \cdots & \cdots & \cdots & \cdots \\ \Omega_{\tau_1}^{(r-1)}, & \Omega_{\tau_2}^{(r-1)}, & \cdots, & \Omega_{\tau_r}^{(r-1)} \end{vmatrix}, \tag{8}$$

where the upper index is used to designate the relative conjugates. When two of the subscripts τ are alike the expression (8) vanishes. Where no two are alike the determinant factor in (8) is, aside from sign, the same for all determinants of the matrix, and hence the determinant

$$|\Omega_{\tau_k}^{(s)}|$$

must be a common factor of all the determinants of the matrix. Moreover, all the numbers of the ideal product $O_1 \cdot O_2 \cdot O_3 \cdots O_r$ can be represented linearly by means of the products

$$\pi = i_{\lambda_1\tau_1} \cdot i_{\lambda_2\tau_2} \cdots i_{\lambda_r\tau_r}$$

and hence the greatest common factor of the products π must be a factor of the product $O_1 \cdot O_2 \cdots O_r$. But each π is divisible by $O_1 \cdot O_2 \cdots O_r$, there being in π one number from each of these ideals, and hence their highest common factor must be divisible by $O_1 \cdot O_2 \cdots O_r$. Thus $O_1 \cdot O_2 \cdot O_2 \cdots O_r$ is itself the highest common factor of the products π, and hence the relative discriminant of K is

$$D_k = O_1^2 \cdot O_2^2 \cdot O_3^2 \cdots O_r^2 \, | \, \Omega_{\tau_k}^{(i)} |^2,$$

which is an ideal in the subfield k. Since $\Omega_\tau^{(i)} = \bar{\Omega}_\tau^{(i)} / D_k(\vartheta)$ we can write

$$D_k = \frac{O_2^2 \cdot O_3^2 \cdots O_r^2}{D_k(\vartheta)^{2r-2}} \, | \, \bar{\Omega}_\tau^{(i)} |^2$$

remembering that O_1 is the principal ideal $[D_k(\vartheta)]$. Again since

$$\bar{\Omega}_\tau^{(i)} = A_1 + A_2 \vartheta^{(i)} + \cdots + \vartheta^{(i)^{r-1}},$$

we have

$$D_k = \frac{O_2^2 \cdot O_3^2 \cdots O_r^2}{D_k(\vartheta)^{2r-2}} D_k(\vartheta).$$

If as before we put $D_k(\vartheta) / O_r = I_r$, we have

$$D_k = \frac{D_k(\vartheta)}{I_2^2 \cdot I_3^2 \cdots I_r^2}.$$

It is easily seen from the previous deduction that the ideals $I_1, I_2, \cdots, I_r$ are those factors of the relative discriminant of ϑ for which as moduli ϑ is the root of a congruence of lower degree than r in k.

The Discriminant of a Field Formed by the Composition of Two Fields.

We shall next make an application of the relative discriminant of a field in the form found above to determine the nature of the discriminant of a field formed by the composition of two fields, in the case where the degree of the compounded field is equal to the product of the degrees of the two fields from which it is formed, divided by the degree of their greatest common subfield.

The problem of the composition of fields has been studied by HENSEL,* but his results are of a different nature from those obtained by the method here used.

I shall suppose that the field K of degree N is formed by composition from the two fields k_1 and k_2, of degrees n_1 and n_2 respectively. Moreover, let κ be the greatest common subfield to k_1 and k_2 and let the degree of κ be ν. If we let P_1 and P_2 be the degrees of k_1 and k_2 relative to κ, and r_1 and r_2 the degrees of K relative to k_1 and k_2, respectively, we have

$$n_1 = \nu P_1, \qquad n_2 = \nu P_2, \qquad N = r_1 n_1 = r_2 n_2.$$

* HENSEL: *Journal für die reine und angewandte Mathematik*, vol. 105 (1889), p. 329; vol. 120 (1899), p. 99.

But by hypothesis $N = n_1 \cdot n_2/\nu = P_2 n_1$. From this and $N = r_1 n_1$ we conclude that $r_1 = P_2$, and in the same way $r_2 = P_1$. Therefore $N = r_1 \cdot r_2 \cdot \nu$.

I shall indicate by D, d_1, d_2, δ respectively the discriminants of K, k_1, k_2, κ, and the relative discriminant by using as subscript the symbol of the field relative to which it is taken. I shall, moreover, indicate by $N_1(\ )$, $N_2(\ )$, $N(\ )$ the norms taken respectively in the fields k_1, k_2, κ and by N_{k_1}, N_{k_2}, N_κ the relative norms.

From what we have seen above we know that $r_1 \cdot r_2$ is the relative degree of K with respect to κ.

If now α_2 is a number which determines k_2, then α_2 will determine K relative to k_1, and we can therefore write

$$D_{k_1} = \frac{O_{12}^2 \cdot O_{13}^2 \cdots O_{1r_1}^2}{D_{k_1}(\alpha_2)^{2r_1-2}} D_{k_1}(\alpha_2), \tag{9}$$

$$d_{2\kappa} = \frac{O_2^2 \cdot O_3^2 \cdots O_{r_1}^2}{D_\kappa(\alpha_2)^{2r_1-2}} D_\kappa(\alpha_2), \tag{10}$$

where $d_{2\kappa}$ is the relative discriminant of k_2 with respect to κ. But since $P_2 = r_1$ we have

$$D_\kappa(\alpha_2) = D_{k_1}(\alpha_2),$$

because the equation in k_1, which α_2 satisfies, is then the same as the equation in κ, the subfield of k_1. Now $O_{1\tau}$ is an ideal in k_1 and O_τ is an ideal in κ, and since κ is a subfield of k_1 from the definition of $O_{1\tau}$ and O_τ, it follows that O_τ is contained in $O_{1\tau}$ and, hence, $O_{1\tau}$ is a factor of O_τ. Hence $D_\kappa(\alpha_2)/O_\tau = I_\tau$ is a factor of $D_\kappa(\alpha_2)/O_{1\tau} = I_{1\tau}$. If we therefore put

$$\frac{I_{12} \cdot I_{13} \cdots I_{1r_1}}{I_2 \cdot I_3 \cdots I_{r_1}} = T,$$

we see that T contains all the ideal factors of $D_\kappa(\alpha_2)$ in k_1 for which α_2 will satisfy a congruence of degree less than r_1 in k_1 but not in the κ.

Hence from (9) and (10)

$$d_{2\kappa} = T^2 D_{k_1}.$$

Taking the norm in k_1, we get

$$N_1(d_{2\kappa}) = N_1(T^2) N_1(D_{k_1}),$$

or since $d_{2\kappa}$ is an ideal in κ,

$$N(d_{2\kappa}^{r_2}) = N_1(T^2) \cdot N_1(D_{k_1}).$$

But then from the known relation

$$d_2 = \delta^{r_1} N(d_{2\kappa}) \tag{11}$$

* BACHMANN, *Allgemeine Arithmetik der Zahlenkörper*, 2.

we have

$$\frac{d_2^{r_2}}{\delta^{r_1 r_2}} = N_1(T^2) \cdot N_1(D_{k_1}). \tag{12}$$

Similar to (11) we have (Bachmann, loc. cit.)

$$D = d_1^{r_1} \cdot N_1(D_{k_1}),$$

and from this we finally have

$$D = \frac{d_1^{r_1} \cdot d_2^{r_2}}{\delta^{r_1 r_2} \cdot N_1(T^2)}. \tag{13}$$

From (12) we see that every prime factor of $N_1(T^2)$ must be a factor of d_2, and if in the previous work we interchange α_1 and α_2, and k_1 and k_2 we should get another ideal T' and $N_2(T'^2)$ would be such that every prime factor of this would be a factor of d_1. But as in either case the final result (13) would have to be the same, we see that

$$N_1(T^2) = N_2(T'^2),$$

and this therefore contains only such prime factors as are common to d_1 and d_2.

URBANA, ILL.