

# A NEW DEVELOPMENT OF THE THEORY OF ALGEBRAIC NUMBERS\*

BY

G. E. WAHLIN

## INTRODUCTION

In volume 144 of *Crelle's Journal* Hensel gave a new development of the theory of quadratic domains of rationality. This development suggested to me a similar treatment of the general algebraic domain of degree  $n$ , which I wish to present in the following pages.

Let us suppose that we have an irreducible equation  $F(x) = 0$ , with integral rational coefficients and of degree  $n$ . Let  $\alpha$  be one of its roots. Since there is no loss in generality in assuming that  $\alpha$  is an algebraic integer we shall do so. Thus the coefficients of  $F(x)$  are all integers and the leading coefficient is unity.

As the construction and the development of the ring  $R(g, \alpha)$  can be accomplished in the same way as was done by Professor Hensel, by simply replacing the fundamental system  $1, \xi$  of the quadratic domain by the fundamental system  $\omega_1, \omega_2, \dots, \omega_n$  of the domain  $k(\alpha)$ , of degree  $n$ , we shall omit the discussion and refer the reader to § 1 of Professor Hensel's article.

It is however of fundamental importance in the following development to know that in  $R(g)$ , the ring of the rational  $g$ -adic numbers, the number  $\alpha$  cannot satisfy an equation of degree less than  $n$ , and I shall therefore prove this, before taking up the further study of the domain determined by  $\alpha$ .

Suppose that

$$\phi(x) = a_0 x^{n-1} + a_1 x^{n-2} + \dots + a_{n-1}$$

is a polynomial of degree less than  $n$ , with  $g$ -adic coefficients, such that  $\phi(\alpha) = 0(g)$ , and let

$$\alpha^{i-1} = a_{i1} \omega_1 + a_{i2} \omega_2 + \dots + a_{in} \omega_n \quad (i = 1, 2, \dots, n).$$

We then have

$$\phi(\alpha) = \mathfrak{A}_1 \omega_1 + \mathfrak{A}_2 \omega_2 + \dots + \mathfrak{A}_n \omega_n,$$

$$\mathfrak{A}_i = a_0 a_{ni} + a_1 a_{n-1i} + \dots + a_{n-1} a_{1i} \quad (i = 1, 2, \dots, n).$$

---

\* Presented to the Society, April 2, 1915.

Since an integer of  $k(\alpha)$  is divisible by  $g$  when and only when each coefficient in its representation by a fundamental system is a multiple of  $g$ , we conclude that  $\phi(\alpha) = 0(g)$  when and only when  $\mathfrak{A}_i = 0(g)$  ( $i = 1, 2, \dots, n$ ), and from this system of equations it follows that  $|a_{ij}| \cdot a_k = 0(g)$ .

But the  $a_{ik}$  are ordinary rational integers and hence  $|a_{ij}|$  is a number of  $k(1)$  and since it is not zero there exists a number  $1/|a_{ij}| \neq 0$  and

$$\frac{1}{|a_{ij}|} \cdot |a_{ij}| \cdot a_k = a_k = 0(g).$$

Hence  $\phi(x)$  must vanish identically, and  $\alpha$  cannot in  $R(g)$  satisfy an equation of degree less than  $n$ .

Since the further results of § 1 of Professor Hensel's article may, without difficulty, be extended to the case under consideration, we shall pass on to the study of the ring  $R(p, \alpha)$  where  $p$  is a rational prime.

#### 1. THE RING $R(p, \alpha)$ WHEN $F(x)$ IS IRREDUCIBLE IN $k(p)$

From the theory of the rational numbers we know that when  $p$  is a prime, the  $p$ -adic numbers constitute a domain which we denote by  $k(p)$ .

We have assumed that  $F(x)$  is irreducible in the ordinary sense, and shall next see that when it is irreducible in  $k(p)$  the ring  $R(p, \alpha)$  is also a domain which, as such, shall be denoted by  $k(p, \alpha)$ .

To prove this it is sufficient to show that if  $\beta \neq 0(p)$  then every equation of the form  $\beta \cdot x = \gamma(p)$  has a unique solution, and as this is true if  $\beta x = 1(p)$  has a unique solution, we need only show that every number which is different from zero in  $R(p, \alpha)$  has a unique reciprocal.

Since  $\beta$  is a number of  $R(p, \alpha)$  it is a rational integral function  $B(\alpha)$  of  $\alpha$ , with rational  $p$ -adic coefficients, and of degree less than  $n$ . Since  $F(x)$  is irreducible in  $k(p)$ ,  $F(x)$  and  $B(x)$  are relatively prime. Moreover, since  $k(p)$  is a domain and hence permits the use of Euclid's algorithm, there exist functions  $M(x)$  and  $N(x)$  such that

$$M(x) \cdot F(x) + N(x) \cdot B(x) = 1(p).$$

Since  $F(\alpha) = 0$  and  $B(\alpha) = \beta$ , we have  $N(\alpha) \cdot \beta = 1(p)$ . Hence  $\beta$  has a reciprocal in  $R(p, \alpha)$ . This reciprocal is moreover unique, because if  $\beta_1$  and  $\beta_2$  are two numbers such that  $\beta \cdot \beta_1 = \beta \cdot \beta_2 = 1(p)$ , then  $\beta\beta_1 - \beta\beta_2 = \beta(\beta_1 - \beta_2) = 0(p)$  and hence  $\beta_1\beta(\beta_1 - \beta_2) = \beta_1 - \beta_2 = 0(p)$ . Therefore  $\beta_1 = \beta_2(p)$  and  $R(p, \alpha)$  is a domain.

The further study of this domain has been carried out by Professor Hensel in Chapter 6, §§ 3, 4, of his *Theorie der Algebraischen Zahlen*, and we shall therefore omit any further discussion of it.

2. THE RING  $R(p, \alpha)$  WHEN  $F(x)$  IS REDUCIBLE IN  $k(p)$ 

I have shown in the introduction that  $\alpha$  cannot in  $k(p)$  satisfy an equation of degree less than  $n$ . If we therefore suppose that

$$F(x) = F_1(x) \cdot F_2(x) \cdots F_s(x) \quad (p),$$

where  $F_1(x), F_2(x), \dots, F_s(x)$  are irreducible in  $k(p)$ , we have

$$F_1(\alpha) \cdot F_2(\alpha) \cdots F_s(\alpha) = 0 \quad (p),$$

while no one of the factors is zero. We therefore conclude that in this case  $R(p, \alpha)$  is not a domain.

Since  $F(x)$  is irreducible in the ordinary sense its discriminant cannot vanish and hence it must also be different from zero for the domain of  $p$ . Consequently no two of the  $s$  factors can be equal.

We shall now introduce, corresponding to each of the  $s$  factors of  $F(x)$ ,  $s$  new systems of values for the numbers of  $R(p, \alpha)$  as follows. If  $\beta = B(\alpha)$  is any number of  $R(p, \alpha)$  and if

$$B(x) = Q_i(x) \cdot F_i(x) + R_i(x) \quad (p),$$

we shall call  $R_i(\alpha)$  the value of  $\beta$  for the domain of  $\mathfrak{p}_i$  corresponding to the factor  $F_i(x)$  and shall write  $\beta = R_i(\alpha) (\mathfrak{p}_i)$ .

Two numbers  $\beta_1 = B_1(\alpha)$  and  $\beta_2 = B_2(\alpha)$  are said to be equal for the domain of  $\mathfrak{p}_i$  when and only when  $B_1(x) - B_2(x)$  is divisible by  $F_i(x)$ .

We thus have  $s$  new rings  $R(\mathfrak{p}_i, \alpha)$  ( $i = 1, 2, \dots, s$ ) such that each number of  $R(p, \alpha)$  is for the domain of  $\mathfrak{p}_i$  equal to some number of  $R(\mathfrak{p}_i, \alpha)$  and the sum, difference, and product of two numbers of  $R(p, \alpha)$  is for the domain of  $\mathfrak{p}_i$  equal to the sum, difference, and product respectively of the corresponding numbers of  $R(\mathfrak{p}_i, \alpha)$ . Evidently  $F_i(\alpha) = 0 (\mathfrak{p}_i)$ .

We shall next see that these  $\mathfrak{p}_i$ -adic values of the numbers of  $R(p, \alpha)$  constitute a domain. As before we need only show that every number  $\beta \neq 0 (\mathfrak{p}_i)$  has a uniquely determined reciprocal in  $R(\mathfrak{p}_i, \alpha)$ .

Let us therefore suppose that  $\beta = B(\alpha) \neq 0 (\mathfrak{p}_i)$ . Since  $\beta \neq 0 (\mathfrak{p}_i)$  it follows that  $B(x)$  is not divisible by  $F_i(x)$  and hence since  $F_i(x)$  is irreducible we know that they are relatively prime. Hence there are two polynomials  $\psi_i(x)$  and  $\phi_i(x)$  such that

$$\phi_i(x) \cdot F_i(x) + \psi_i(x) \cdot B(x) = 1 \quad (p),$$

and since rational numbers are equal for the domain of  $\mathfrak{p}_i$  if they are equal for the domain of  $p$ , we can write

$$\phi_i(x) \cdot F_i(x) + \psi_i(x) \cdot B(x) = 1 \quad (\mathfrak{p}_i),$$

the coefficients of the polynomials being rational numbers. But

$$F_i(\alpha) = 0 \quad (\mathfrak{p}_i)$$

and hence  $\psi_i(\alpha) \cdot \beta = 1 \quad (\mathfrak{p}_i)$ . Therefore  $\beta$  has a reciprocal which in the same way as before can be shown to be unique. Hence the  $\mathfrak{p}_i$ -adic values of the numbers of  $R(p, \alpha)$  form a domain which we shall denote by  $k(\mathfrak{p}_i, \alpha)$ .

If two numbers  $\beta_1 = B_1(\alpha)$  and  $\beta_2 = B_2(\alpha)$  of  $R(p, \alpha)$  are equal for each of the domains  $\mathfrak{p}_i$  ( $i = 1, 2, \dots, s$ ) then they are equal for the domain of  $p$ . For, if  $\beta_1 = \beta_2 \quad (\mathfrak{p}_i)$  ( $i = 1, 2, \dots, s$ ) then  $B_1(x) - B_2(x)$  is divisible by  $F_i(x)$  ( $i = 1, 2, \dots, s$ ) and since these factors are distinct it must be divisible by their product. But  $B_1(x) - B_2(x)$  is of degree less than  $n$  and hence this is possible only when  $B_1(x) = B_2(x) \quad (p)$  and hence  $\beta_1 = \beta_2 \quad (p)$ .

Conversely, if  $\beta_1 = \beta_2 \quad (p)$ , then  $\beta_1 = \beta_2 \quad (\mathfrak{p}_i)$  ( $i = 1, 2, \dots, s$ ). For, since  $B_1(\alpha) - B_2(\alpha) = 0 \quad (p)$  and since  $\alpha$  cannot in  $k(p)$  satisfy an equation of degree less than  $n$  we conclude that  $B_1(x) - B_2(x) = 0 \quad (p)$ , and hence  $B_1(x) - B_2(x)$  is divisible by each of the functions  $F_i(x)$  and  $\beta_1 = \beta_2 \quad (\mathfrak{p}_i)$  ( $i = 1, 2, \dots, s$ ).

Since  $F_1(x), F_2(x), \dots, F_s(x)$  are all irreducible and distinct, the product  $F_1(x) \cdot F_2(x) \cdots F_{i-1}(x) \cdot F_{i+1}(x) \cdots F_s(x)$  is not divisible by  $F_i(x)$  and hence

$$F_1(\alpha) \cdot F_2(\alpha) \cdots F_{i-1}(\alpha) \cdot F_{i+1}(\alpha) \cdots F_s(\alpha) \neq 0 \quad (\mathfrak{p}_i).$$

Hence there exists in  $R(p, \alpha)$  a number  $\psi_i(\alpha)$  such that

$$\chi_i(\alpha) = \psi_i(\alpha) \cdot F_1(\alpha) \cdots F_{i-1}(\alpha) \cdot F_{i+1}(\alpha) \cdots F_s(\alpha) = 1 \quad (\mathfrak{p}_i)$$

and as is easily seen  $\chi_i(\alpha) = 0 \quad (\mathfrak{p}_j)$  ( $j \neq i$ ). If we now put  $\beta_{\mathfrak{p}_i} = \beta \cdot \chi_i(\alpha)$ , where  $\beta$  is any number of  $R(p, \alpha)$ , we have

$$\beta_{\mathfrak{p}_i} = \beta \quad (\mathfrak{p}_i), \quad \beta_{\mathfrak{p}_i} = 0 \quad (\mathfrak{p}_j) \quad (j \neq i),$$

$$\beta = \sum_{i=1}^s \beta_{\mathfrak{p}_i} \quad (\mathfrak{p}_i) \quad (i = 1, 2, \dots, s),$$

and hence

$$\beta = \sum_{i=1}^s \beta_{\mathfrak{p}_i} \quad (p).$$

Moreover if from each of the domains  $k(\mathfrak{p}_i, \alpha)$  we choose a number  $\beta_i = B_i(\alpha)$  and put

$$B(x) = \sum_{i=1}^s B_i(x) \chi_i(x)$$

and  $\beta = B(\alpha) \quad (p)$ , then  $\beta = \beta_i \quad (\mathfrak{p}_i)$  ( $i = 1, 2, \dots, s$ ). Hence for arbitrarily chosen  $\beta_i$  there exists in  $R(p, \alpha)$  a number  $\beta$  such that  $\beta = \beta_i \quad (\mathfrak{p}_i)$ .

If we now let  $\beta_i$  be the  $\mathfrak{p}_i$ -adic value of an arbitrarily chosen number  $\beta$  of  $R(p, \alpha)$ , and put  $\beta_1, \beta_2, \dots, \beta_{i-1}, \beta_{i+1}, \dots, \beta_s$  each equal to 1, then there exists in  $R(p, \alpha)$  a number  $\bar{\beta}_{\mathfrak{p}_i}$  such that

$$\bar{\beta}_{\mathfrak{p}_i} = \beta_i \quad (\mathfrak{p}_i) \quad (i = 1, 2, \dots, s)$$

and hence

$$\beta = \prod_{j=1}^s \bar{\beta}_{\mathfrak{p}_j} \quad (\mathfrak{p}_i) \quad (i = 1, 2, \dots, s)$$

and therefore

$$\beta = \prod_{j=1}^s \bar{\beta}_{\mathfrak{p}_j} \quad (p).$$

### 3. CERTAIN RELATIVE DOMAINS

In order to complete the study of the domains  $k(\mathfrak{p}_i, \alpha)$  introduced in the preceding section it will be necessary to take up a brief discussion of certain relative domains.

Let us denote by  $n_i$  the degree of  $F_i(x)$  and by  $\delta_i$  the order of its discriminant. Let  $r$  be a rational integer greater than  $\max(\delta_1, \delta_2, \dots, \delta_s)$ . The polynomial whose coefficients are the  $r$ th convergents of the coefficients of  $F_i(x)$  we shall denote by  $F_i^{(r)}(x)$ , and the roots of the equation  $F_i^{(r)}(x) = 0$  by  $\alpha_{i1}^{(r)}, \alpha_{i2}^{(r)}, \dots, \alpha_{in_i}^{(r)}$ .

From Chapter 4, § 3, of Hensel's *Theorie der Algebraischen Zahlen*, we know that  $F_i^{(r)}(x)$  is irreducible in  $k(p)$  and hence the domains  $k(p, \alpha_{ij}^{(r)})$  ( $i = 1, 2, \dots, s; j = 1, 2, \dots, n_i$ ) are of the kind considered above in § 1.

Moreover in  $k(p, \alpha_{ij}^{(r)})$  the equation

$$F_i(x) = 0 \quad (p)$$

has a solution\* which we shall denote by  $\alpha_{ij}$ .

Let us next suppose that

$$f_{ij}(x) = 0 \quad (p)$$

is the equation of lowest degree in  $k(p, \alpha_{ij}^{(r)})$  which  $\alpha$  satisfies. We shall next see that at least one of the functions  $f_{i1}(x), f_{i2}(x), \dots, f_{in_i}(x)$  has, in the domain to which it belongs, the corresponding linear factor  $x - \alpha_{ij}$ .

Since  $F(\alpha) = 0 \quad (p)$ , we know that the degree of  $f_{ij}(x)$  is less than or equal to  $n$ . Let us denote this degree by  $\nu_{ij}$ . We can then write

$$F(x) = Q_{ij}(x) \cdot f_{ij}(x) + R_{ij}(x) \quad (p),$$

where  $R_{ij}(x)$  is of degree less than  $\nu_{ij}$ . Thus

$$R_{ij}(\alpha) = 0 \quad (p),$$

---

\* Hensel, *Theorie der Algebraischen Zahlen*, p. 159.

and hence  $R_{ij}(x)$  must vanish identically. Hence  $f_{ij}(x)$  must be a factor of  $F(x)$ . Since

$$F(x) = F_1(x) \cdots F_s(x) \quad (p),$$

we see that  $F(\alpha_{ij}) = 0 \quad (p)$  and hence  $x - \alpha_{ij}$  is a factor of  $F(x)$  in  $k(p, \alpha_{ij}^{(r)})$ .

Let us next suppose that no one of the functions  $f_{ij}(x)$  is divisible by the corresponding linear factor  $x - \alpha_{ij}$ . Let us moreover put

$$\phi_{ij}(x) = \frac{F(x)}{x - \alpha_{ij}}.$$

Then since  $f_{ij}(x)$  and  $x - \alpha_{ij}$  are relatively prime and  $k(p, \alpha_{ij}^{(r)})$  is a domain, we can find  $M(x)$  and  $N(x)$  such that

$$M(x) \cdot f_{ij}(x) + N(x) \cdot (x - \alpha_{ij}) = 1 \quad (p),$$

and therefore

$$M(x) \cdot f_{ij}(x) \cdot \phi_{ij}(x) + N(x) \cdot F(x) = \phi_{ij}(x) \quad (p).$$

But  $F(x)$  is divisible by  $f_{ij}(x)$  and from the last equation we conclude that  $\phi_{ij}(x)$  is divisible by  $f_{ij}(x)$  and hence

$$\phi_{ij}(\alpha) = 0 \quad (p) \quad (j = 1, 2, \dots, n_i).$$

If we now put

$$\psi_i(x) = \sum_{j=1}^{n_i} \phi_{ij}(x),$$

$\alpha$  is a root of the equation  $\psi_i(x) = 0 \quad (p)$ . But

$$\psi_i(x) = \sum_{j=1}^{n_i} \frac{F(x)}{x - \alpha_{ij}} = \frac{F(x)}{F_i(x)} \cdot F'_i(x),$$

which has rational coefficients and is of degree  $n - 1$ . But we already know that, in  $k(p)$ ,  $\alpha$  cannot satisfy an equation of degree less than  $n$ . The assumption that no  $f_{ij}(x)$  has a linear factor therefore leads to a contradiction.

We can therefore suppose that  $f_{i1}(x)$  is divisible by  $x - \alpha_{i1}$  in  $k(p, \alpha_{i1}^{(r)})$ . Then as in § 2 we conclude that  $R(p, \alpha_{i1}^{(r)}, \alpha)$  is not a domain and in the same manner we can introduce new systems of values, corresponding to the various irreducible factors of  $f_{i1}(x)$  in  $k(p, \alpha_{i1})$ . These, we can show, form domains. We shall denote by  $k(\mathfrak{p}_{i1}, \alpha_{i1}^{(r)}, \alpha)$  the particular domain corresponding to the factor  $x - \alpha_{i1}$ . In the same manner as in § 2, it then follows that  $\alpha = \alpha_{i1}(\mathfrak{p}_{i1})$ .

By this equation we have established a correspondence between the numbers of  $k(\mathfrak{p}_i, \alpha)$  and those of  $k(p, \alpha_{i1}^{(r)})$ , the corresponding numbers being equal for the domain of  $\mathfrak{p}_{i1}$ .

The sum, product, difference, and quotient, of two numbers of  $k(\mathfrak{p}_i, \alpha)$  correspond to the sum, product, difference, and quotient, respectively, of the corresponding numbers of  $k(p, \alpha_{i1}^{(r)})$ .

If  $\mathfrak{A}_1$  and  $\mathfrak{A}_2$  are rational numbers from  $k(\mathfrak{p}_i, \alpha)$  and  $k(p, \alpha_{i1}^{(r)})$  respectively and if  $\mathfrak{A}_1$  corresponds to  $\mathfrak{A}_2$  then, as is easily seen,  $\mathfrak{A}_1 = \mathfrak{A}_2(p)$ . If  $\beta$  is any number of  $k(\mathfrak{p}_i, \alpha)$  and  $\bar{\beta}$  the corresponding number of  $k(p, \alpha_{i1}^{(r)})$  and if  $f(x) = 0(p)$  is the irreducible equation in  $k(p)$  which  $\bar{\beta}$  satisfies then  $f(\bar{\beta}) = 0(p)$  and hence  $f(\beta) = 0(\mathfrak{p}_i)$ .

If we now define an integer of  $k(\mathfrak{p}_i, \alpha)$  to be a number which for the domain of  $\mathfrak{p}_i$  satisfies an irreducible equation with rational integral coefficients and the leading coefficient unity, we see that to an integer of  $k(\mathfrak{p}_i, \alpha)$  corresponds an integer of  $k(p, \alpha_{i1}^{(r)})$  and to a prime number of  $k(p, \alpha_{i1}^{(r)})$  corresponds a prime number of  $k(\mathfrak{p}_i, \alpha)$ .

By the norm  $N_{\mathfrak{p}_i}(\beta)$  of a number of  $k(\mathfrak{p}_i, \alpha)$  we shall understand the norm of the corresponding number of  $k(p, \alpha_{i1}^{(r)})$ .

By means of these definitions and the correspondence thus established, the results of the development of the domain  $k(p, \alpha_{i1}^{(r)})$  as given by Professor Hensel (see § 1) are seen at once to be true for the domains  $k(\mathfrak{p}_i, \alpha)$ .

The theory of divisors in Professor Hensel's paper can now without trouble be extended to the general case.