and $p^2 f_1 g_1$ is divisible by p^t, where $t = 2 + 2s - 2\rho > s + 1$. We choose $\rho_1(x)$ so that the degree of $f_1(x)$ shall be less than the degree of $f_0(x)$; then by (20) the degree of $g_1(x)$ will be less than the degree of $g_0(x)$.

Similarly, if in accord with (18) we set

$$F^{(s+1)} - (f_0 + pf_1)(g_0 + pg_1) = p^{s+2}(L_2 - F_{s+2}),$$

the congruence

$$F^{(s+2)} \equiv (f_0 + pf_1 + p^2 f_2)(g_0 + pg_1 + p^2 g_2) \pmod{p^{s+3}}$$

is satisfied if we take

$$f_2 \equiv p^{s-\rho}(bL_2 - \rho_2 f_0), \quad g_2 \equiv p^{s-\rho}(aL_2 + \rho_2 g_0) \pmod{p^{s+1}}.$$

The general step in the proof may now be made as in § 2.

HENSEL'S THEORY OF ALGEBRAIC NUMBERS.

Theorie der Algebraischen Zahlen. Von KURT HENSEL. Erster Band. Leipzig and Berlin, Teubner, 1908. xi + 346 pp.

IN the theory of functions one may investigate an analytic function in the neighborhood of a point $z = a$ by means of a power series in $z - a$. In arithmetic one usually employs only developments according to the fixed base 10. The author undertakes in the present work to introduce a corresponding mobility into arithmetic and algebra by employing expansions of numbers into power series in an arbitrary prime number p.

A positive integer D can be expressed in one and but one way in the form

$$D = d_0 + d_1 p + \cdots + d_k p^k,$$

in which each d_i is one of the integers $0, 1, \cdots, p - 1$. This equation will be said to define the representation of D as a p-adic number, for which the following symbol will be employed:

$$D = d_0, d_1 d_2 \cdots d_k \ (p).$$

For example,

$$14 = 2 + 3 + 3^2 = 2{,}11 \ (3), \quad 216 = 2 \cdot 3^3 + 2 \cdot 3^4 = 0{,}0022 \ (3).$$

The sum of two such p-adic numbers is readily expressed as a p-adic number. For example,

$$0{,}0022 + 0{,}1021 = 0{,}10111 \ (3).$$

When $A \geqq B$, the difference $A - B$ is expressible as a p-adic number. Thus, if $A = 216$, $B = 138$, $p = 3$, we have

$$0{,}0022 - 0{,}1021 = 0{,}222 \quad (3).$$

But if $A < B$ a similar rule for subtraction (proceeding from left to right and borrowing when necessary unity from a later digit) would lead to an infinite sequence of digits. For example, if we take $p = 3$ and attempt to subtract, in this manner, 0,0022 from 0,1021, we obtain $0{,}10022\cdots$, in which the digit 2 is to be repeated indefinitely. It would be useless to define this symbol involving an infinitude of digits to be the infinite series

$$3 + 2\cdot 3^4 + 2\cdot 3^5 + \cdots + 2.3^n + \cdots,$$

which is divergent and not equal to 138–216. On the contrary we shall attach no numerical significance to such a symbol. Our procedure will be analogous to that employed in basing a theory of positive fractions upon the theory of positive integers by introducing symbols (a, b) involving a pair of integers. We here introduce symbols called p-adic numbers and define equality and the four rational operations. We shall prove that our set of p-adic numbers is closed under these operations and hence forms a field or domain. A certain subset of these p-adic numbers can be put into one-to-one correspondence with the rational numbers such that the sum, difference, product, or quotient of two p-adic numbers corresponds to the sum, etc., of the corresponding rational numbers. We shall then have a representation of each rational number as a p-adic number.

We note that, for $p = 3$, the quotient of $1 + 2\cdot 3 + 3^2$ by 3 is $3^{-1} + 2 + 3$, which is conveniently denoted by the symbol 12,1 (3).

Accordingly we introduce the symbols, called p-adic numbers,

$$D = d_{-\rho}\, d_{-\rho+1}\cdots d_{-1}\, d_0,\ d_1\, d_2\cdots \quad (p),$$

in which there is a finite number of *coefficients* d_i preceding the comma and a finite number or an infinitude of coefficients following the comma, while each d_i is a rational number in whose expression as a fraction in its lowest terms the denominator is not divisible by p. Such a fraction a/b is called *integral modulo* p since it plays the same rôle modulo p as the unique inte-

gral root of the congruence $bx \equiv a \pmod{p}$. A *reduced* p-adic number is one all of whose coefficients are integers of the set $0, 1, \cdots, p-1$.

For $k \geqq -\rho$, the rational number

$$D_k = d_{-\rho}p^{-\rho} + \cdots + d_{-1}p^{-1} + d_0 + d_1 p + \cdots + d_k p^k$$

is called the *convergent* D_k *of rank* k of the p-adic number D. For $k < -\rho$, we set $D_k = 0$. Thus if $D = 12{,}1\ (3)$, $D_{-1} = 3^{-1}$, $D_0 = 3^{-1} + 2$.

Two rational numbers will be called congruent modulo p^m if their difference equals the product of p^m by a number which is integral modulo p. Here m may be zero or any positive or negative integer. For example,

$$4\cdot 5^{-2} \equiv \tfrac{2}{3}\cdot 5^{-2} \pmod{5^{-1}}, \quad 9\cdot 5^{-2} \equiv \tfrac{2}{3}\cdot 5^{-2} \pmod{5^0},$$

since

$$4\cdot 5^{-2} - \tfrac{2}{3}\cdot 5^{-2} = \tfrac{2}{3}\cdot 5^{-1}, \quad 9\cdot 5^{-2} - \tfrac{2}{3}\cdot 5^{-2} = \tfrac{1}{3},$$

while $\frac{2}{3}$ and $\frac{1}{3}$ are integral modulo 5.

Two p-adic numbers D and D' are said to be *equal* when for every integer k their convergents D_k and D'_k of rank k are congruent modulo p^{k+1}. Note that $D_k \equiv D'_k \pmod{p^{k+1}}$ implies $D_l \equiv D'_l \pmod{p^{l+1}}$ for every $l < k$. For example,

$$D = p, p-1\, p-1\, p-1 \cdots, \quad D' = 0$$

are equal since

$$D_k = p + (p-1)p + \cdots + (p-1)p^k = p^{k+1}, \quad D'_k = 0.$$

In particular, two reduced p-adic numbers are equal if and only if their corresponding coefficients are identical. Every p-adic number equals a reduced p-adic number. The proof follows from the fact that any rational number which is integral modulo p can be expressed in the form $i + lp$, where i is one of the integers $0, 1, \cdots, p-1$, and l is integral modulo p. For example,

$$1\tfrac{2}{3},0 = 14{,}1313 \cdots (5)$$

with the repetend 13, since

$$\tfrac{2}{3} = 4 + (-\tfrac{2}{3})5, \quad -\tfrac{2}{3} = 1 + (-\tfrac{1}{3})5, \quad -\tfrac{1}{3} = 3 + (-\tfrac{2}{3})5.$$

If we prefix one or more zeros before a p-adic number D, we

obtain a p-adic number equal to D. Given any two p-adic numbers D and D', we may prefix enough zeros before one so that we obtain two numbers with the same number ρ of coefficients to the left of the comma. Then the *sum* of D and D' is defined to be the p-adic number

$$D + D' = d_{-\rho} + d'_{-\rho} \cdots d_{-1} + d'_{-1} \;\; d_0 + d'_0, \;\; d_1 + d'_1 \cdots (p).$$

For example, $10,12 + 0,211 = 10,012$ (3). If $D = D_1$ and $D' = D'_1$, then $D + D'$ equals $D_1 + D'_1$.

The unique p-adic number X for which $X + D' = D$ is called the difference $D - D'$. Hence

$$D - D' = d_{-\rho} - d'_{-\rho} \cdots d_{-1} - d'_{-1} \;\; d_0 - d'_0, \;\; d_1 - d'_1 \cdots (p).$$

For example, employing a bar to denote a repetend, we have

$$0,\overline{12} - 0,\overline{210} = 0,\overline{201002} \quad (3).$$

The product P of two p-adic numbers D and D' is defined to be the p-adic number whose coefficients are those in the series obtained by the formal multiplication of the series

$$d_{-\rho} p^{-\rho} + \cdots + d_{-1} p^{-1} + d_0 + d_1 p + \cdots,$$
$$d'_{-\rho'} p^{-\rho'} + \cdots + d'_{-1} p^{-1} + d'_0 + d'_1 p + \cdots.$$

In particular, if D and D' are *integral* p-adic numbers,

$$D = d_0, \; d_1 d_2 \cdots, \quad D' = d'_0, \; d'_1 d'_2 \cdots (p),$$

their product is

$$P = d_0 d'_0, \quad d_0 d'_1 + d_1 d'_0 \quad d_0 d'_2 + d_1 d'_1 + d_2 d'_0 \cdots (p).$$

In general, $P = c_{-\gamma} c_{-\gamma+1} \cdots$, where $\gamma = \rho + \rho'$ and

$$c_{-\gamma} = d_{-\rho} d'_{-\rho'}, \quad c_{-\gamma+1} = d_{-\rho} d'_{-\rho'+1} + d_{-\rho+1} d'_{-\rho'}, \quad \cdots.$$

If the c's and d's are given numbers integral modulo p and d_ρ is not a multiple of p, the preceding equations uniquely determine each d' as a number integral modulo p, so that the quotient P/D is uniquely determined as a p-adic number $D' = d'_{\rho-\gamma} \cdots$. In particular, if D is a reduced p-adic number other than zero, P/D equals a p-adic number. For example,

$$3,12 \div 4,21 = 2,\overline{4220} \quad (5).$$

If $D = D_1$ and $D' = D'_1$, then $DD' = D_1 D'_1$ and $D/D' = D_1/D'_1$.

For addition and multiplication as defined above the commutative, associative and distributive laws are seen to hold. The totality of p-adic numbers forms a field or Körper $K(p)$, being closed under the above defined operations addition, subtraction, multiplication, and division (the divisor not being equal to zero).

Any rational number $\neq 0$ may be given the form

$$r = \frac{a}{b} \cdot p^n,$$

where n is zero or a positive or negative integer, while a and b are integers not divisible by p. To r we make correspond the *monomial* p-adic number all but one of whose coefficients are zero, that one being a/b and occupying the n-th place to the right of the comma if n is positive, and the $(1-n)$-th place to the left of the comma if n is zero or negative. To the rational number zero we make correspond the p-adic number zero. The product or quotient of two rational numbers r and r' obviously corresponds to the product or quotient of the corresponding monomial p-adic numbers. A like result is seen to hold for the sum or difference, if we make use of the fact that the monomial p-adic number with the coefficient $p^k d$ in the n-th place equals a monomial with the coefficient d in the $(k+n)$-th place. These monomial p-adic numbers when expressed as reduced p-adic numbers are periodic, and conversely any periodic p adic number equals a monomial (Hensel, page 38). Hence the set of all periodic reduced p-adic numbers is simply isomorphic with the domain of all rational numbers. The p-adic number, whether reduced or not, which corresponds to the rational number r will be designated $[r]$.

Any p-adic number $E = e_0, e_1 e_2 \cdots$, in which e_0 is not a multiple of p, is called a *unit* for the domain $K(p)$. Hence any p-adic number D can be expressed as a product $[p^n]E$. The exponent n is zero or a positive or negative integer and is called the *order* of D. The product or quotient of two units is a unit. The order of a product is the sum of the orders of the factors. A p-adic number $D = [p^n]E$ is called integral if its order n is positive or zero, and fractional if n is negative.

Consider an integral function of a variable x

$$f(x) = A_0 x^n + A_1 x^{n-1} + \cdots + A_n$$

with p-adic coefficients A_i. If $A_i^{(k)}$ is the convergent of rank k of A_i, the function with rational coefficients

$$f^{(k)}(x) = A_0^{(k)}x^n + \cdots + A_n^{(k)}$$

is called the convergent of rank k of $f(x)$. Two integral functions $f(x)$ and $g(x)$ with p-adic coefficients are called equal if, for every integer k, their convergents $f^{(k)}(x)$ and $g^{(k)}(x)$ are congruent modulo p^{k+1}, namely, if the coefficients of like powers of x are congruent.

An integral function is called reducible or irreducible in the domain $K(p)$ according as it is or is not equal to the product of two integral functions, each of degree $\geqq 1$, with p-adic coefficients.

Any integral function $f(x)$ can be expressed as a product of a p-adic number and a *primary* function

$$F(x) = [p^a]x^n + B_1x^{n-1} + \cdots + B_n$$

whose coefficients are integral p-adic numbers not all divisible by p, that of the highest power of x corresponding to a power of p. The product of two primary functions is primary. It is readily seen that $f(x)$ is reducible if and only if its primary component $F(x)$ is the product of two primary functions.

In case the discriminant $D(F)$ of $F(x)$ is zero, $F(x)$ and its derivative $F'(x)$ have a common factor which can be determined by Euclid's process. We may therefore restrict our attention to a primary function $F(x)$ whose discriminant is not zero and hence is of the form $[p^\delta]E$, where $\delta \geqq 0$. Then (Hensel, page 68) $F(x)$ is reducible if and only if its convergent $F^{(\delta)}(x)$ is reducible modulo $p^{\delta+1}$. A similar argument (page 71) shows that if

$$F(x) \equiv f(x)g(x) \pmod{p^{r+1}}$$

and $r + 1 > 2\rho$, where ρ is the order of the p-adic number defined by the resultant of $f(x)$ and $g(x)$, then $F(x)$ is reducible in $K(p)$. An important special case is the following. If

$$F(x) \equiv f(x)g(x) \pmod{p},$$

where f and g have no common factor modulo p, then $F(x)$ is reducible in $K(p)$. Since

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-\overline{p-1}) \pmod{p},$$

we conclude that $x^{p-1} - 1$ has $p - 1$ linear factors in $K(p)$, so that there exist $p - 1$ p-adic numbers which are $(p - 1)$-th roots of unity. They are all powers of a primitive $(p - 1)$-th root of unity, designated by ω. For example,

$$\omega = 2,22\cdots (3), \quad \omega = 3,46\cdots (7).$$

Any p-adic number can be expressed in the form

$$B = p^{\rho}\omega^{\beta}e,$$

where e is a principal unit $1, a_1a_2\cdots (p)$. If μ is not divisible by p, B is the μ-th power of a p-adic number if and only if ρ is divisible by μ and β is divisible by the greatest common divisor d of μ and $p - 1$ (page 87). In particular if p is odd, $\sqrt[\mu]{B}$ is a p-adic number only when ρ and β are both even. For example, $\sqrt{2}$ is not a 3-adic number, since $2 = \omega e$; while $\sqrt{2}$ is a 7-adic number, since $2 = \omega^2 e$. For p an odd prime, B is the p-th power of a p-adic number if and only if ρ is divisible by p and e is of the form $1, 0e_2e_3\cdots (p)$.

A number β is called algebraic if it is the root of at least one equation

$$x^m + B_1x^{m-1} + \cdots + B_m = 0 \tag{1}$$

with rational coefficients. If $B_1,\cdots, B_m$ are integers, the root β is called an integral algebraic number. If $B_1,\cdots, B_m$ are rational numbers which are integral modulo p, β is called an algebraic number integral modulo p. If β and γ are algebraic numbers integral modulo p then $\beta + \gamma$, $\beta - \gamma$ and $\beta\gamma$ are algebraic numbers integral modulo p. The roots of an equation

$$x^r + \beta_1x^{r-1} + \cdots + \beta_r = 0,$$

whose coefficients are algebraic numbers integral modulo p, are algebraic numbers integral modulo p.

If in (1) each $B_i = b_i/p^{\rho}$ where b_i is integral modulo p, then $\gamma = p^{\rho}\beta$ is a root of

$$\gamma^m + b_1\gamma^{m-1} + p^{\rho}b_2\gamma^{m-2} + \cdots p^{\rho(m-1)}b_m = 0.$$

Hence every algebraic number β can be given the form γ/p^{ρ} where γ is an algebraic number integral modulo p, and ρ is an integer $\geqq 0$.

Let α be an algebraic number and let

$$F(x) = x^\lambda + a_1 x^{\lambda-1} + \cdots + a_\lambda = 0 \tag{2}$$

be the equation irreducible in the domain of rational numbers which has the root α. The totality of the rational functions of α with rational coefficients forms a field $K(\alpha)$ of *degree* λ. As shown in the theory of algebraic numbers, there exist λ integral algebraic numbers $\gamma_1, \cdots, \gamma_\lambda$ of $K(\alpha)$ such that every algebraic number γ of $K(\alpha)$ can be expressed in one and but one way in the form

$$\gamma = u_1\gamma_1 + u_2\gamma_2 + \cdots + u_\lambda\gamma_\lambda, \tag{3}$$

where each u_i is a rational number, while every integral algebraic number is of the form (3), where now each u_i is an integer. The numbers $\gamma_1, \cdots, \gamma_\lambda$ are said to form a fundamental system for $K(\alpha)$. Since $\beta + \gamma$ and $\beta\gamma$ are algebraic numbers integral modulo p when β and γ are, it follows that

$$v_1\gamma_1 + \cdots + v_\lambda\gamma_\lambda \tag{4}$$

is an algebraic number integral modulo p if $v_1, \cdots, v_\lambda$ are rational numbers integral modulo p. Conversely (Hensel, page 121), any algebraic number integral modulo p can be given the form (4).

An algebraic number β is said to be divisible by p^ρ if $\beta = p^\rho\gamma$, where γ is integral modulo p. If $\beta = b_1\gamma_1 + \cdots$, the conditions are $b_i \equiv 0 \pmod{p^\rho}$, for $i = 1, \cdots, \lambda$.

Two algebraic numbers are called congruent modulo p^ρ if $\beta - \beta'$ is divisible by p^ρ. The conditions are $b_i \equiv b_i' \pmod{p^\rho}$ for $i = 1, \cdots, \lambda$.

If β is integral modulo p, so that each b_i is a rational number integral modulo p, we can determine integers e_i of the set $0, 1, \cdots, p-1$ such that $b_i = e_i + pc_i$, where c_i is integral modulo p. Hence $\beta = \epsilon + p\gamma$, where

$$\epsilon = e_1\gamma_1 + \cdots + e_\lambda\gamma_\lambda, \ \gamma = c_1\gamma_1 + \cdots + c_\lambda\gamma_\lambda.$$

A number of the type ϵ is called a reduced number of $K(\alpha)$. Hence any algebraic number integral modulo p is congruent modulo p to a reduced number.

Just as we introduced a field $K(p)$ of all p-adic numbers containing a sub-field simply isomorphic with the field of all rational numbers, so we shall now introduce a field containing

a sub-field simply isomorphic with $K(\alpha)$. To this end we employ the symbols

$$\delta = \delta_{-\rho} \cdots \delta_{-1}\delta_0, \ \delta_1\delta_2 \cdots \quad (p),$$

called p-adic algebraic numbers, in which each δ_i is an algebraic number of $K(\alpha)$ integral modulo p. When each δ_i is a reduced number ϵ_i, δ is called a reduced p-adic algebraic number. By the convergent of rank μ of δ is meant

$$\delta^{(\mu)} = \delta_{-\rho} p^{-\rho} + \cdots + \delta_{-1} p^{-1} + \delta_0 + \delta_1 p + \cdots + \delta_\mu p^\mu,$$

which is a number of the domain $K(\alpha)$. Two p-adic algebraic numbers δ and γ are called equal if, for every integer μ, their convergents of rank μ are congruent modulo $p^{\mu+1}$. In particular, if δ and γ are reduced, they are equal only when corresponding coefficients δ_i and γ_i are identical. In view of the preceding paragraph, any p-adic algebraic number β equals a reduced p-adic algebraic number.

Addition and multiplication of p-adic algebraic numbers is defined as for p-adic numbers. The totality of p-adic algebraic numbers based upon $K(\alpha)$ is seen to form a field $K(p, \alpha)$.

Any number $\beta \neq 0$ of $K(\alpha)$ can be expressed in one and but one way in the form $\beta = \gamma p^n$, where γ is a number of $K(\alpha)$ integral modulo p and not divisible by p, while n is zero or a positive or negative integer. To β we make correspond the monomial p-adic algebraic number all but one of whose coefficients are zero, that one being γ and occupying the nth place to the right of the comma if n is positive, and the $(1 - n)$-th place to the left if n is zero or negative. When this monomial is expressed as a reduced p-adic algebraic number its coefficients $\epsilon_n, \epsilon_{n+1}, \cdots$, form a periodic series. This follows from the fact that in (3) each u_i is rational and hence is represented by a periodic p-adic number. Hence $K(\alpha)$ is simply isomorphic to the sub-field of $K(p, \alpha)$ composed of the periodic reduced p-adic algebraic numbers. The p-adic algebraic number, whether reduced or not, which corresponds to the number β of $K(\alpha)$ will be designated $[\beta]$.

In the p-adic algebraic number δ, each coefficient δ_i is a linear function of $\gamma_1, \cdots, \gamma_\lambda$. Hence the convergent $\delta^{(\mu)}$ equals $u_1^{(\mu)}\gamma_1 + \cdots + u_\lambda^{(\mu)}\gamma_\lambda$, in which $u_i^{(\mu)}$ is the convergent of order μ of a p-adic number u_i. Hence

$$\delta = u_1[\gamma_1] + \cdots + u_\lambda[\gamma_\lambda]. \tag{5}$$

Let the function (2) with the root α be expressed as a product

$$F(x) = F_1(x)\,F_2(x)\cdots F_t(x) \quad (p) \tag{6}$$

in which $F_i(x)$ has p-adic coefficients, is irreducible in $K(p)$ and is of degree λ_i. Let $\alpha_1 = [\alpha]$, $\alpha_2, \cdots, \alpha_{\lambda_1}$ be the roots of $F_1(x) = 0$.

Since the number γ_i of $K(\alpha)$ equals a rational function of α with rational coefficients, it follows from (5) that

$$\delta = \phi(\alpha_1) \quad (p),$$

where ϕ is a rational function with p-adic coefficients. Thus

$$\delta_j = \phi(\alpha_j) \qquad (j = 1, \cdots, \lambda_1)$$

are the roots of the equation

$$g_1(y) = \pi(y - \delta_j) = y^{\lambda_1} + b_1 y^{\lambda_1 - 1} + \cdots + b_\lambda = 0 \quad (p), \tag{7}$$

with p-adic coefficients. If $g_1(y)$ has a factor $f(y)$ irreducible in $K(p)$ which vanishes for $y = \delta_1$, then $f[\phi(x)] = 0$ has one root α_1 in common with the equation $F_1(x) = 0$ irreducible in $K(p)$ and hence has all the roots of the latter, so that $f(y)$ vanishes for each δ_i. Hence the various irreducible factors of $g_1(y)$ have the same roots and are therefore identical. Thus $g_1(y)$ is either irreducible or a power of an irreducible function. Multiplying $g_1(y)$ by a suitable power of p, we obtain

$$G_1(y) = B_0 y^{\lambda_1} + B_1 y^{\lambda_1 - 1} + \cdots + B_{\lambda_1} = 0 \quad (p), \tag{7'}$$

where the B_i are integral p-adic numbers not all divisible by p. It follows (Hensel, pages 74, 75) that B_0 and B_{λ_1} are not both divisible by p. Hence either δ or $1/\delta$ satisfies an equation with integral p-adic coefficients. A root of such an equation is said to be algebraically integral. A p-adic algebraic number ϵ is called an algebraic unit if both ϵ and $1/\epsilon$ are algebraically integral.

The product $\delta_1 \cdots \delta_{\lambda_1}$ is called the partial norm $n_1(\delta)$ of $\delta = \delta_1$ with respect to the factor $F_1(x)$. Since

$$n_1(\delta) = (-1)^{\lambda_1} B_{\lambda_1}/B_0$$

is an integral p-adic number only when B_0 is not divisible by p, we conclude that δ is algebraically integral if and only if $n_1(\delta)$ is an integral p-adic number. In particular, ϵ is an algebraic unit if and only if $n_1(\epsilon)$ and its reciprocal are integral

p-adic numbers, namely, if $n_1(\epsilon)$ is a p-adic unit E. The product or quotient of two algebraic units is therefore a unit.

If δ and β are p-adic algebraic numbers, such that δ/β is algebraically integral, δ is said to be divisible by β. The condition is that $n_1(\delta)/n_1(\beta)$ shall be an integral p-adic number and hence that the order of $n_1(\delta)$ shall be equal to or greater than the order of $n_1(\beta)$. In case these orders are equal, δ/β is an algebraic unit ϵ and δ and β are said to be equivalent.

The norms $n_1(\delta)$ of all algebraically integral numbers δ not units, are of the form p^dE, where $d > 0$. Let f_1 be the least integer d, and π_1 a number for which

$$n_1(\pi_1) = p^{f_1}E. \tag{8}$$

If π is another number whose norm has the order f_1, then $\pi = \pi_1\epsilon$ so that π and π_1 are equivalent. Every algebraically integral number δ not a unit is divisible by π_1 since $d \geqq f_1$. In particular, π_1 has no divisor other than itself and the units ϵ. If the product of two algebraically integral numbers is divisible by π_1, one of the factors is divisible by π_1. For, if neither δ nor δ' is divisible by π_1, each is a unit and hence $\delta\delta'$ is a unit and not divisible by π_1. Hence π_1 has the characteristic properties of a prime number, and all the primes in $K(p, \alpha)$ are equivalent. Since $n_1(p) = p^{\lambda_1}$, π_1 is a divisor of p.

If β is any number of $K(p, \alpha)$, $n_1(\beta) = p^bE$. Set

$$b = \rho_1 f_1 + f_0, \quad 0 \leqq f_0 < f_1.$$

Then $\beta' = \beta/\pi_1^{\rho_1}$ has the norm $p^{b-\rho_1 f_1}E' = p^{f_0}E'$. Hence $f_0 = 0$, so that β' is a unit ϵ. Hence every number β of $K(p, \alpha)$ is of the form $\beta = \epsilon\pi_1^{\rho_1}$. Here ρ_1 is called the order of β; it is the quotient of the order of $n_1(\beta)$ by f_1. In particular, $p = \epsilon\pi_1^{e_1}$, where $e_1 = \lambda_1/f_1$.

Two numbers β and β' of $K(p, \alpha)$ are called congruent modulo π_1^r if $\beta - \beta'$ is divisible by π_1^r. Hence if β is integral there is a reduced number $\epsilon^{(0)}$ such that

$$\beta \equiv \epsilon^{(0)} \pmod{\pi_1}, \quad \beta = \epsilon^{(0)} + \pi_1\beta^{(1)}.$$

Similarly, $\beta^{(1)} = \epsilon^{(1)} + \pi_1\beta^{(2)}$, etc. Hence

$$\beta \equiv \epsilon^{(0)} + \epsilon^{(1)}\pi_1 + \epsilon^{(2)}\pi_1^2 + \cdots + \epsilon^{(k)}\pi_1^{(k)} \pmod{\pi_1^{k+1}}.$$

Any number δ of $K(p, \alpha)$ is of the form $\pi_1^{\rho_1}\epsilon$. Taking $\beta = \epsilon$, we obtain the congruence

$$\delta \equiv \epsilon^{(\rho_1)}\pi_1^{\rho_1} + \epsilon^{(\rho_1+1)}\pi_1^{\rho_1+1} + \cdots + \epsilon^{(k)}\pi_1^{(k)} \pmod{\pi_1^{k+1}}. \tag{9}$$

We have $\pi_1^{e_1} = p\epsilon$ where ϵ is a unit of $K(p, \alpha)$. Thus

$$\pi_1 = p^{1/e_1}\epsilon_1,$$

where $\epsilon_1 = \epsilon^{1/e_1}$ is an algebraic unit not belonging in general to $K(p, \alpha)$. Extending our definition of equivalence, we write

$$\pi_1 \sim p^{1/e_1}. \tag{10}$$

If we replace α_1 by another root α_i of $F_1(x) = 0$, π_1 is replaced by a prime equivalent to p^{1/e_1} and hence to π_1. Hence in view of (9) we obtain symbolical developments of the conjugate numbers $\delta(\alpha_i)$ in power series in p^{1/e_1}. These are analogous to the power series in $(z - \alpha)^{1/e_1}$ for the roots of an algebraic equation in the neighborhood of a branch point $z = \alpha$ of order e_1.

For another factor $F_i(x)$ in (6) we have primes

$$\pi_i \sim p^{1/e_i},$$

where e_i is a divisor of the degree λ_i of F_i. In order to avoid speaking of different, but equivalent, prime numbers, we associate with the factor $F_i(x)$ a unique prime divisor $\mathfrak{p}_i$ and say that a p-adic algebraic number δ is divisible by $\mathfrak{p}_i^{\rho_i}$ and by no higher power of $\mathfrak{p}_i$ if $\delta = \epsilon\pi_i^{\rho_i}$, so that the development, analogous to (9), begins with $\pi_i^{\rho_i}$. Thus p has the distinct prime divisors $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$. Every number γ of $K(\alpha)$ is therefore divisible by definite powers of these prime divisors. Then $\gamma\gamma'$ and γ/γ' are divisible by exactly the powers $\rho_i + \rho_i'$ and $\rho_i - \rho_i'$ of $\mathfrak{p}_i$. A number γ is algebraically integral if and only if it contains no one of the prime divisors $\mathfrak{p}_i$ to a negative power.

If $x_1, \cdots, x_{\lambda_i}$ are the roots of $F_i(x) = 0$, then

$$\delta_j = \phi(x_j) \quad (j = 1, \cdots, \lambda_i)$$

are the roots of $g_i(y) = 0$, an equation analogous to (7). Thus

$$g(y) = g_1(y) \cdots g_t(y)$$

is a function whose constant term c_n differs at most in sign from the complete norm $n(\delta)$ which equals the product $n_1(\delta) \cdots n_t(\delta)$ of the partial norms of δ. Let now δ be an integral number of $K(\alpha)$. Then the coefficients of $g(y)$ are rational integers since its roots are $\phi(\beta)$ where β ranges over all the roots of (2). The highest power of p dividing $n(\delta)$ is p^d, where $d = \rho_1 f_1 + \cdots + \rho_t f_t$. But an integer c_n has only a finite number of prime factors. Hence an integral algebraic number γ has only a finite number of prime divisors.

In terms of these prime divisors, Hensel obtains (pages 214–237) an expression for the discriminant of $K(\alpha)$, that is, the discriminant of any fundamental system. Further he determines (pages 261–280) the conditions under which the discriminants of the various numbers of $K(\alpha)$ have a common unessential divisor. Hensel here makes an important advance in the theory of algebraic numbers. For other important results the reader is referred to the text itself.

In a book of the original character of the present one, some minor defects may be expected and excused. On page 16, A/B need not be, as stated, one of the integral p-adic numbers $c_0, c_1, \cdots$. At the middle of page 34 occurs an equation, although equality of two fractional p-adic numbers has not yet been defined. If A, B, C are integral or fractional p-adic numbers such that $A = BC$, and if A_k, B_k, C_k are their convergents of rank k, it is stated on page 36 that

$$B_k \cdot C_k \equiv A_k \pmod{p^{k+1}}.$$

While this is true for integral p-adic numbers, it is in general false for fractional p-adic numbers. For if B is of negative order $-b$, and C of order $-c$, and $b \geqq c$, we must employ the convergent of rank $k + b$ of C in order to reach all the terms of the convergent of rank k of A. The above congruence holds for the modulus p^{k+1-b}. On page 69, fourth line below (7), greater than p^ρ should be equal to or greater than p^ρ; the proof is however valid. On page 96, before (2), read among all equations with rational coefficients. On page 121, fifth line from bottom, $v_i - v_i^{(0)}$ should have the denominator p. On page 123, the context shows the meaning of the term algebraically divisible; in the paragraph following (2), ganze should be preceded by modulus p, while $\bar{u}_i = p^\delta \bar{u}_i$ contains a misprint. In the eleventh line on page 124, the final letter p should be $\gamma^{(\lambda)}$. In the fifth line on page 135, B_λ should be B_0. In the theorem on page 161, the term Bereich occurs in two senses; in the first instance it should be $K(p, \alpha)$, in the second, $K(p)$. On page 326, negative powers of p may occur in the p-adic development of B.

In the above exposition of the elements of Hensel's theory, I have avoided Hensel's notation $\Sigma_{i=-\rho}^{\infty} c_i p^i$ for a p-adic number, and have not identified the rational numbers with their corresponding p-adic representations. The terms greater than and less than as applied to p-adic numbers (Hensel, page 19) are not

in accord with the usage for real numbers, so that if the rational numbers a, b correspond to the p-adic numbers $[a]$, $[b]$, we may have $a > b$, $[a] < [b]$. In setting up this correspondence, I have introduced the term monomial p-adic number. On page 130, Hensel assumes that the equation for α is irreducible in $K(p)$. Although not stated explicitly, this assumption underlies §§ 3–7 of the same chapter. In the present account I have therefore avoided this assumption and proceeded at once with the general case; see (6) above.

In addition to the intrinsic interest attached to the new fields or domains introduced by Hensel, his theory has proved to be of such importance in the difficult problems relating to discriminants that it must be granted a permanent footing in the theory of algebraic numbers.

L. E. DICKSON.

UNIVERSITY OF CHICAGO,
May 9, 1910.

SHORTER NOTICES.

Factor Table for the First Ten Millions. By D. N. LEHMER. Washington, D. C., Carnegie Institution of Washington, 1909. xiv + 476 pp.

THE publication of Lehmer's factor table marks an event of the greatest importance in the science of higher arithmetic. The chief factor tables published hitherto are the following: For the first, second and third millions, Burckhardt (Paris, 1817, 1814, 1816); fourth, fifth and sixth millions, Glaisher (London, 1879, 1880, 1883); seventh, eighth and ninth millions, Dase and Rosenberg (Hamburg, 1862, 1863, 1865). Rosenberg's manuscript for the tenth million was presented by his widow to the Berlin Academy of Sciences, but has disappeared. Crelle's manuscript for the third, fourth, and fifth millions was turned over to the Berlin Academy but was found to be too inaccurate for publication. Kulik's manuscripts, placed in charge of the Vienna Royal Academy in 1867 (see Encyklopädie der Mathematischen Wissenschaften, volume I, page 951; *Wiener Berichte,* volume 53, page 460) purport to give the smallest factor of all numbers up to one hundred million which are not divisible by 2, 3, or 5. In Kulik's manuscript each prime not exceeding 163 is represented by a