

## 剩餘類域的特徵數爲 $p$ 的完全的分立賦值域

聶 靈 沼

(北 京 大 學)

一完全的，分立賦值域  $K$  的結構基本上由其剩餘類域  $\mathfrak{K}$  決定，此首由 H. Hasse 與 F. K. Schmidt 證明。今就  $\mathfrak{K}$  的特徵數爲質數的情況，本文給以一簡單而一致的證明。並且由於  $\mathfrak{K}$  的正規代表系的獲得，致使  $K$  的結構當  $\mathfrak{K}$  爲非完成域時 ( $\mathfrak{K}' \neq \mathfrak{K}$ ) 更爲清楚。

---

## DISCRETE-VALUED COMPLETE FIELDS WITH RESIDUE CLASS FIELDS OF CHARACTERISTIC $p$

BY NIEH LING CHAO

*Peking University*

### INTRODUCTION

It was first discovered by H. Hasse and F. K. Schmidt<sup>1</sup> that a discrete-valued, complete field  $K$  is essentially determined by its residue class field  $\mathfrak{K}$ . Later on, E. Witt<sup>2</sup> gave a much simpler proof for the case that  $\mathfrak{K}$  is perfect of characteristic  $p$ , and an indirect proof for the imperfect case was given by O. Teichmüller<sup>3</sup>. Our aim here is to give a unified proof for both cases, so that the structure of  $K$  will become clear in the imperfect case. First we give a simple method for constructing a minimal discrete-valued, complete field  $K$  with a given  $\mathfrak{K}$  as its residue class field. (Part I) In the construction, we obtain naturally a “regular representative

- 
1. H. Hasse und F. K. Schmidt, Die Struktur diskret bewerteter Körper, Crelle, 170 (1936).
  2. E. Witt, Zyklische Körper und Algebren der Charakteristik  $p$  von Grad  $p^n$ , Crelle, 176 (1936).
  3. O. Teichmüller, Diskret bewertete perfekte Körper mit unvollkommen Restklassen-körper, Crelle, 176 (1936).

system", which is a generalization of Teichmüller's multiplicative representative system that played an important rôle in Witt's work. In virtue of the existence of such a representative system, we prove easily that  $K$  can be imbedded analytically in a given discrete-valued, complete field with the same residue class field  $\mathfrak{K}$ . (Part II)

### I. EXISTENCE THEOREM

Let  $\mathfrak{K}$  be a field of characteristic  $p > 0$ .

LEMMA 1 (TEICHMÜLLER)<sup>4</sup>. *If  $\mathfrak{K}$  is imperfect, then  $\mathfrak{K}$  contains a  $p$ -basis  $\mathfrak{M}$ , i.e., a subset  $\mathfrak{M}$  of  $\mathfrak{K}$  with the following properties:*

a) *If  $c_1, \dots, c_r$  are any  $r$  distinct elements of  $\mathfrak{M}$ , then  $\mathfrak{K}^p(c_1 \cdots c_r)$  has degree  $p^r$  over the subfield  $\mathfrak{K}^p$  of all  $p$ -th powers of elements of  $\mathfrak{K}$ .*

b)  $\mathfrak{K}^p(\mathfrak{M}) = K$ .

It follows from a) that

c) *If  $c_1, \dots, c_r$  are any  $r$  distinct elements of  $\mathfrak{M}$ , then any relation  $c_1^{e_1} \cdots c_r^{e_r} = 1$  implies all  $e_i = 0$ .*

We make the convention that the null set is regarded as the  $p$ -basis of every perfect field  $\mathfrak{K}$ .

Let  $\mathfrak{M}^*$  denote the set consisting of the unity element  $e$  of  $\mathfrak{K}$  and all products  $c_1^{e_1} \cdots c_r^{e_r}$ , where  $0 \leq e_i \leq p-1$  ( $i=1, \dots, r$ ) and  $c_1, \dots, c_r$  are distinct elements of a  $p$ -basis  $\mathfrak{M}$  of  $\mathfrak{K}$ . By properties a) and b)  $\mathfrak{M}^*$  forms a linear basis of  $\mathfrak{K}$  over  $\mathfrak{K}^p$ , i.e., Every element  $a$  of  $\mathfrak{K}$  may be uniquely written as a linear combination of elements  $b_i$  of  $\mathfrak{M}^*$  with coefficients  $a_i^p$  from  $\mathfrak{K}^p$ :

$$1) \quad a = \sum_i a_i^p b_i.$$

(1) is called the system of fundamental relations of  $\mathfrak{K}$  with respect to the  $p$ -basis  $\mathfrak{M}$ .

Let  $\bar{\mathfrak{M}}$  denote the set of all products  $c_1^{e_1} \cdots c_r^{e_r}$ ,  $e_i \geq 0$  ( $i=1, \dots, r$ ),  $c_1, \dots, c_r \in \mathfrak{M}$ .

4. O. Teichmüller,  $p$ -Algebren, Deutsche Mathematik 1 (1936).

It is clear that  $\mathfrak{M}^* \subset \mathfrak{M}$ , as  $\mathfrak{M}$  is non-empty.

By the Binomial theorem we can easily prove

**LEMMA 2.** *Let  $\mathfrak{a}$  and  $\mathfrak{b}$  be any two ideals in a commutative ring. If for all  $\alpha$  of  $\mathfrak{a}$  both  $\alpha^p$  and  $p\alpha$  belong to  $\mathfrak{b}$ , then the congruence  $x \equiv y \pmod{\mathfrak{a}}$  implies  $x^p \equiv y^p \pmod{\mathfrak{b}}$ .*

Let  $\Gamma$  be the ring of rational integers, and let  $\Pi$  be the prime field of characteristic  $p$ . Let  $f(x)$  and  $f(x^{p^n})$  denote polynomials  $f(x_1, \dots, x_m)$  and  $f(x_1^{p^n}, \dots, x_m^{p^n})$  in the polynomial ring  $\Gamma[x_1, \dots, x_m]$  of  $m$  independent indeterminates  $x_1, \dots, x_m$  over  $\Gamma$ . If  $f(\xi^{p^i}) = f(\xi_1^{p^i}, \dots, \xi_m^{p^i}) = 0$  ( $i \geq 0$ ,  $\xi_1^{p^i}, \dots, \xi_m^{p^i}$  in  $\Pi$  or an extension of  $\Pi$ ), we shall say that  $f(x)$  has a zero  $\xi^{p^i}$ .

**LEMMA 3.** *Let  $S$  be the set of all polynomials of  $\Gamma[x_1, \dots, x_m]$ , which have a common zero in an extension of  $\Pi$ , and let  $\mathfrak{a}_n$  ( $n=0, 1, 2, \dots$ ) denote the ideal of  $\Gamma[x_1, \dots, x_m]$  generated by all  $p^n f(x)$ ,  $p^{n-1} f(x)^p, \dots, f(x)^{p^n}$  for  $f(x)$  in  $S$ . Then  $p^n$  does not belong to  $\mathfrak{a}_n$ .*

*Proof.* Let  $x_1 = \xi_1, \dots, x_m = \xi_m$  be the common zero, and write  $\mathfrak{a}_n = \mathfrak{a}_n(\xi)$ . Let us assume that  $p^n$  belongs to  $\mathfrak{a}_n(\xi)$  for some  $n > 0$ , namely,

$$2) \quad p^n = \sum_{i=0}^n \sum_{j=1}^r X_{i,j}(x) \cdot p^i f_j(x)^{p^{n-i}},$$

for  $f_j(x)$  in  $S$  and  $X_{i,j}(x)$  in  $\Gamma[x_1, \dots, x_m]$ . We shall prove that then  $p^{n-1}$  belongs to  $\mathfrak{a}_{n-1}(\xi^{p^{-n}})$ . Substituting  $x_i^{p^n}$  for  $x_i$  in (2), we get

$$p^n = \sum_{i=0}^n \sum_{j=1}^r X_{i,j}(x^{p^n}) \cdot p^i f_j(x^{p^n})^{p^{n-i}}.$$

But  $\sum_{i=1}^n \sum_{j=1}^r X_{i,j}(x^{p^n}) \cdot p^{i-1} f_j(x^{p^n})^{p^{n-i}} = F$ ,  $F$  belongs clearly to the ideal  $\mathfrak{a}_{n-1}(\xi^{p^{-n}})$ . Since each  $X_{0,j}(x^{p^n})$  may be written as a sum of  $p^n$ -th powers of elements of  $\Gamma[x_1, \dots, x_m]$ , the summation  $\sum_{j=1}^r X_{0,j}(x^{p^n}) f_j(x^{p^n})^{p^n}$  may also be written as a sum of  $p^n$ -th powers  $\sum_{i=1}^s F_i(x)^{p^n}$  such that each  $F_i(x)$  is a multiple of some  $f_j(x^{p^n})$ . So,

$$3) \quad p^n = \sum_{i=1}^s F_i(x)^{p^n} + p F.$$

By an elementary theorem,

$$4) \quad \sum_{i=1}^s F_i(x)^{p^n} = \left( \sum_{i=1}^s F_i(x) \right)^{p^n} - \sum_{\substack{v_1 + \dots + v_s = p^n \\ v_i < p^n}} \frac{p^n!}{v_1! \dots v_s!} F_1(x)^{v_1} \dots F_s(x)^{v_s}.$$

For each term  $\frac{p^n!}{v_1! \dots v_s!} F_1(x)^{v_1} \dots F_s(x)^{v_s}$ , let  $p^r$  be the highest power of  $p$  which divides all  $v_i$ . Put  $v_i = t p^r$  and  $Q = \frac{(p^n-1)!}{(v_1-1)! \dots (v_s-1)!} \frac{1}{t}$ , without loss of generality, we may assume  $(t, p) = 1$ . Since both  $Q p^{n-r} = \frac{p^n!}{v_1! \dots v_s!}$  and  $Q t = \frac{(p^n-1)!}{(v_1-1)! \dots (v_s-1)!}$  are integers,  $Q$  is an integer. Let  $F_1(x)^{v_1 p^{-r}} \dots F_s(x)^{v_s p^{-r}} = g(x)$ . Then  $g(x)$  is a multiple of some  $f_j(x^{p^n})$ . Since  $v < n$ ,  $Q p^{n-r-1} g(x)^{p^r}$  belongs to  $\alpha_{n-1}(\xi^{p^{-n}})$ . Now  $\frac{p^n!}{v_1! \dots v_s!} F_1(x)^{v_1} \dots F_s(x)^{v_s} = Q p^{n-r} g(x)^{p^r}$ , so the second part in the right side of (4) may be written as  $p G$ ,  $G \in \alpha_{n-1}(\xi^{p^{-n}})$ . From (3) we have

$$5) \quad p^n = \left( \sum_i F_i(x) \right)^{p^n} + p(G + F).$$

Since  $n > 0$ ,  $\sum_i F_i(x)$  together with  $(\sum_i F_i(x))^{p^n}$  is divisible by  $p$ . Let  $\sum_i F_i(x) = p H'$  and  $(\sum_i F_i(x))^{p^n} = p^{p^n} H'^{p^n} = p H$ . Since  $p \geq 2$ ,  $H$  belongs to  $\alpha_{n-1}(\xi^{p^{-n}})$ . From (5),  $p^{n-1} = H + G + F$  belongs to  $\alpha_{n-1}(\xi^{p^{-n}})$ .

Since for any  $\xi$ ,  $\alpha_0(\xi)$  is generated by elements of  $S$ , every element in  $\alpha_0(\xi)$  has  $\xi$  as a zero. But  $\xi$  is not a zero of the constant polynomial 1. So  $1 \notin \alpha_0(\xi)$ . Thus the lemma is true for  $n=0$ , and is true for all  $n$  by induction.

Now we consider an arbitrarily given field  $\mathfrak{K}$  of characteristic  $p > 0$ . We choose arbitrarily a  $p$ -basis  $\mathfrak{M}$  for  $\mathfrak{K}$  and suppose that the linear basis  $\mathfrak{M}^*$ , the set  $\mathfrak{M}$  and the system (1) of fundamental relations of  $\mathfrak{K}$  with respect to the  $p$ -basis  $\mathfrak{M}$  are all defined as above. Moreover, let  $\mathbb{H}$  be the prime field contained in  $\mathfrak{K}$  and  $e$  the unity element of  $\mathfrak{K}$ .

Let  $P$  be a primitive integral domain whose characteristic is divisible

by  $p$ , i.e.,  $P = \Gamma$  or  $P = \Pi$ . Let an indeterminate  $u(x)$  be assigned to each element  $x$  of the union of  $\mathfrak{M}$  and  $\mathfrak{R} - \overline{\mathfrak{M}}$ , except for  $x=0$  and  $x=e$ ; these indeterminates are considered as algebraically independent over  $P$ . Let  $U$  denote the set of all  $u(x)$ . Then the polynomial ring  $P[U]$  is a pure transcendental extension of  $P$ , or  $P$  itself when  $U$  is empty. The latter case occurs only when  $\mathfrak{R}$  is the prime field of characteristic 2. The ring  $P[U]$  is called the *ground ring* of  $\mathfrak{R}$  with respect to the  $p$ -basis  $\mathfrak{M}$ .

In order to construct a discrete-valued, complete field  $K$  with  $\mathfrak{R}$  as its residue class field, we proceed as follows: First we shall introduce an endomorphism  $\sigma$  and a chain of ideals  $\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \dots$  in the ground ring  $P[U]$ . Then we define an exponential valuation  $\omega$  in modified sense on  $P[U]$  by means of the endomorphism and chain of ideals such that all  $x$  of  $P[U]$  with  $\omega(x) = \omega(0)$  form an ideal  $\mathfrak{J}$  in  $P[U]$  and that the quotient ring  $\mathfrak{J} = P[U]/\mathfrak{J}$  is a ring with a valuation in the ordinary sense. The quotient field of the closure of  $\mathfrak{J}$  will be the required field  $K$ .

We define a mapping  $\psi(x)$  of  $\mathfrak{R}$  into  $P[U]$  as follows:

$$6) \quad \psi(0) = 0, \quad \psi(e) = 1,$$

$$7) \quad \psi(x) = u(x) \quad \text{for all } x \in \mathfrak{R} - \overline{\mathfrak{M}},$$

and

$$8) \quad \psi(x) = \prod_i u(c_i)^{e_i} \quad \text{for all } x = \prod_i c_i^{e_i} \in \overline{\mathfrak{M}}, c_i \in \mathfrak{M}.$$

We define the endomorphism  $\sigma$  of  $P[U]$  as follows: For any polynomial  $f(u(x_1), \dots, u(x_m))$  in  $u(x_1), \dots, u(x_m)$  with coefficients in  $P$ , we put

$$9) \quad \sigma(f(u(x_1), \dots, u(x_m))) = f(\sigma(u(x_1)), \dots, \sigma(u(x_m))),$$

and for each  $u(x)$  of  $U$  we make use of the fundamental relation  $a = \sum_i a_i^p b_i$  in the system (1) and define

$$10) \quad \sigma(u(a)) = \sum_i \psi(a_i)^p \psi(b_i).$$

The endomorphism  $\sigma$  is defined as the identity automorphism of  $P[U]$  in case that  $U$  is empty.

Since  $\psi(e) = 1$ , we have  $\sigma(u(c)) = u(c)$  for  $c \in \mathfrak{M}$ . (8) together with (9) implies

$$(11) \quad \sigma(\psi(c)) = \psi(c) \quad \text{for all } c \in \overline{\mathfrak{M}}.$$

When  $\mathfrak{M}$  is non-empty, the product of any two elements  $a$  and  $b$  of  $\overline{\mathfrak{M}}$  is of the form  $c^p d$  with  $c \in \overline{\mathfrak{M}}$  and  $d \in \mathfrak{M}^*$ . From (8) we have

$$(12) \quad \psi(a)\psi(b) = \psi(c)^p \psi(d).$$

Due to (10), the right side in (9) is a polynomial in  $u(x)^p$  for  $x \in \mathfrak{R} - \overline{\mathfrak{M}}$ . Applying the transformation (12) to the expansion of  $\sigma(f(u(x_1), \dots, u(x_m)))$ , we may reduce it to the form

$$\sigma(f(u(x_1), \dots, u(x_m))) = \sum_i \sum_j f_{i,j}^p \psi(b_i)$$

so that all  $b_i$  are distinct elements of  $\mathfrak{M}^*$ . Since  $\sum_j f_{i,j}^p = (\sum_j f_{i,j})^p + p g_i$ , putting  $\sum_j f_{i,j} = f_i$  and  $\sum_i g_i \psi(b_i) = g$ , we obtain finally the form

$$(13) \quad \sigma(f(u(x_1), \dots, u(x_m))) = \sum_i f_i^p \psi(b_i) + p g.$$

Next, we introduce a chain of ideals of  $P[U]$ ,  $\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \dots$  as follows:

Since the characteristic of  $\Pi$  divides that of  $P$ , the mapping  $\alpha \rightarrow \alpha e$ ,  $\alpha \in P$ , is a homomorphism of  $P$  onto  $\Pi$ . Let every polynomial  $f$  of  $P[U]$  be written as the summation  $\sum_{k_1 \dots k_v} \alpha_{k_1 \dots k_v} u(x_1)^{k_1} \dots u(x_v)^{k_v}$  with  $\alpha_{k_1 \dots k_v} \in P$ . Then the mapping  $\tau: f \rightarrow \tau(f) = \sum_{k_1 \dots k_v} \alpha_{k_1 \dots k_v} x_1^{k_1} \dots x_v^{k_v}$  is a homomorphism of  $P[U]$  into  $\mathfrak{R}$ . It is also onto, since the mapping  $\tau$  satisfies the equation

$$(14) \quad \tau(\psi(x)) = x \quad \text{for all } x \in \mathfrak{R}.$$

Let  $\mathfrak{N}$  be the kernel of the homomorphism  $\tau$ . Then the residue class field of  $P[U]$  modulo  $\mathfrak{N}$  is isomorphic with  $\mathfrak{R}$  such that

$$15) \quad \psi(a) + \psi(b) \equiv \psi(a+b) \pmod{\mathfrak{N}}$$

Let  $\mathfrak{q}_n (n=1, 2, 3, \dots)$  denote the ideal of  $P[U]$  generated by all  $S^{p^{n-1}}, pS^{p^{n-2}}, \dots, p^{n-1}S$  for  $S \in \mathfrak{N}$ . It is clear that  $\mathfrak{q}_1 = \mathfrak{N}$  and  $\mathfrak{q}_{n+1} \subseteq \mathfrak{q}_n$  for  $n=1, 2, 3, \dots$ . Since both  $S^p$  and  $pS$  belong to  $\mathfrak{q}_{n+1}$  for all  $S$  of  $\mathfrak{q}_n$ , Lemma 2 holds for each pair  $\mathfrak{a} = \mathfrak{q}_n$  and  $\mathfrak{b} = \mathfrak{q}_{n+1}$  ( $n=1, 2, 3, \dots$ ).

It follows from (1) and (10) that  $\tau(\sigma(u(x))) = \tau(u(x))$  for  $u(x) \in U$ , and in general

$$16) \quad \tau(\sigma(f)) = \tau(f) \quad \text{for all } f \in P[U].$$

In particular,  $\tau(\sigma(S)) = 0$  for  $S \in \mathfrak{N}$ , i.e.,  $\sigma(S)$  together with  $S$  belongs to  $\mathfrak{N}$ . Hence each  $\mathfrak{q}_n$  is invariant under the endomorphism  $\sigma$ .

Further we have to prove some important properties concerning with the endomorphism and the chain of ideals:

$$\text{i) } \sigma^n(f) \equiv \sigma^{n-1}(f) \pmod{\mathfrak{q}_n} \text{ for all } n.$$

Proof. By (16) we have  $\tau(\sigma(f) - f) = 0$ . The lemma is true for  $n=1$  since  $\mathfrak{q}_1 = \mathfrak{N}$ . Let us assume that it is true for  $n$ . Applying  $\sigma^i$  ( $i=n-1, n$ ) to (13), we have

$$\sigma^n(f) = \sum_i \sigma^{n-1}(f_i)^p \psi(b_i) + p \sigma^{n-1}(g),$$

and

$$\sigma^{n+1}(f) = \sum_i \sigma^n(f_i)^p \psi(b_i) + p \sigma^n(g).$$

By Lemma 2,  $\sigma^n(f_i)^p \equiv \sigma^{n-1}(f_i)^p$  and  $p \sigma^n(g) \equiv p \sigma^{n-1}(g) \pmod{\mathfrak{q}_{n+1}}$ . So  $\sigma^{n+1}(f) \equiv \sigma^n(f) \pmod{\mathfrak{q}_{n+1}}$ . i) is thus proved.

$$\text{ii) If } f \text{ belongs to } \mathfrak{q}_n \text{ then } \sigma(f) \equiv p^n \psi(a) \pmod{\mathfrak{q}_{n+1}}.$$

Proof. Let  $\tau(\sigma(f)) = a$ . Since  $\mathfrak{q}_1 = \mathfrak{N}$ ,  $\sigma(f) \equiv \psi(a) \pmod{\mathfrak{q}_1}$  by (14). So the lemma is true for  $n=0$  if we write  $P[U] = \mathfrak{q}_0$ . It is also true for  $n=1$ . For, applying  $\tau$  to (13) we have  $\tau(\sigma(f)) = \sum_i \tau(f_i)^p b_i$ . If  $f$  belongs to  $\mathfrak{q}_1$ , then  $\sigma(f)$  does so also and  $\sum_i \tau(f_i)^p b_i = 0$ . Since all  $b_i$  are distinct elements of the linear basis  $\mathfrak{M}^*$ ,  $\tau(f_i) = 0$ , i.e.,  $f_i \equiv 0 \pmod{\mathfrak{q}_1}$  for

all  $i$ . So  $f_i' \equiv 0 \pmod{q_2}$  for all  $i$ . Let  $g \equiv \psi(a) \pmod{q_1}$ . Then  $\sigma(f) \equiv \rho\psi(a) \pmod{q_2}$ .

Let us assume that ii) is true for  $n-1$  ( $n > 1$ ). In order to show it true for  $n$ , it suffices to show that if  $S$  belongs to  $\mathfrak{N}$  then

$$\sigma(p^i S^{p^{n-1-i}}) \equiv p^n \psi(a_i) \pmod{q_{n+1}}$$

for  $i=0, 1, \dots, n-1$ . Since  $n > 1$ ,  $S^{p^{n-2}}$  belongs to  $q_{n-1}$  and then  $\sigma(S^{p^{n-2}}) \equiv p^{n-1} \psi(a) \pmod{q_n}$ . By Lemma 2,  $\sigma(S^{p^{n-1}}) \equiv p^{(n-1)p} \psi(a)^p \pmod{q_{n+1}}$ . Since  $(n-1)p - n = (n-1)(p-1) - 1 \geq 0$ , we may put  $p^{(n-1)p-n} \psi(a)^p \equiv \psi(b) \pmod{q_1}$ . So  $\sigma(S^{p^{n-1}}) \equiv p^n \psi(b) \pmod{q_{n+1}}$ . For  $i > 0$ ,  $p^{i-1} S^{p^{n-1-i}}$  belongs to  $q_{n-1}$  and therefore  $\sigma(p^{i-1} S^{p^{n-1-i}}) \equiv p^{n-1} \psi(a) \pmod{q_n}$ . Obviously,  $\sigma(p^i S^{p^{n-1-i}}) \equiv p^n \psi(a) \pmod{q_{n+1}}$ . ii) is thus proved.

For the case that  $P$  has the characteristic 0, we have the following properties iii) and iv).

iii) *Let  $P$  be of characteristic 0. If  $p^n f$  belongs to  $q_{n+1}$  for some  $n \geq 0$ , then  $f$  belongs to  $q_1$ . In particular, if  $p^n \psi(a) \equiv p^n \psi(b) \pmod{q_{n+1}}$ , then  $a=b$ .*

*Proof.* Suppose  $f \not\equiv 0 \pmod{q_1}$ . Since  $P[U]/q_1 \cong \mathfrak{R}$ , there is a  $g$  in  $P[U]$  so that  $fg \equiv 1 \pmod{q_1}$ , and  $p^n gf \equiv p^n \pmod{q_{n+1}}$ . If  $\mathfrak{R}$  is the prime field of characteristic 2, then the set  $U$  is empty,  $P[U]=P$  and  $q_n=(p^n)$ . So the lemma is trivial in this case. When the set  $U$  is non-empty, Lemma 3 may be applied. So  $p^n f$  together with  $p^n$  does not belong to  $q_{n+1}$ .

In particular, by (14),  $\psi(a) \equiv \psi(b) \pmod{q_1}$  implies  $a=b$ . Hence iii) is proved.

iv) *Let  $P$  be of characteristic 0. For each element  $f$  of  $P[U]$  there exists a unique sequence  $a_0, a_1, a_2, \dots$  in  $\mathfrak{R}$  such that*

$$(17) \quad \sigma^n(f) \equiv \sigma^n(\psi(a_0) + p\psi(a_1) + \dots + p^n\psi(a_n)) \pmod{q_{n+1}}.$$

*Proof.* By mathematical induction, it follows from ii) that there exists a sequence  $a_0, a_1, a_2, \dots$  in  $\mathfrak{R}$  such that

$$(18) \quad \sigma^n(f) \equiv \sigma^n(\psi(a_0)) + p\sigma^{n-1}(\psi(a_1)) + \dots + p^n\psi(a_n) \pmod{q_{n+1}}.$$



By iii), each element  $a_n$  is uniquely determined by the element  $f$  and the set of all  $a_i$  with  $i < n$ . By induction, the sequence is uniquely determined by the element  $f$ . Due to i), (17) follows from (18).

Now we make use of the endomorphism  $\sigma$  and the chain of ideals  $q_1 \supseteq q_2 \supseteq \dots$  to define a function  $\omega$  on the ground ring  $P[U]$ . Let  $f$  be any element of  $P[U]$ . Then either  $\sigma^n(f) \equiv 0 \pmod{q_{n+1}}$  for all  $n \geq 0$ , or there exists a unique non-negative integer  $r$  such that  $\sigma^n(f) \equiv 0 \pmod{q_{n+1}}$  for all  $n < r$  but  $\sigma^r(f) \not\equiv 0 \pmod{q_{r+1}}$ . In the former case, let  $\omega(f) = \infty$ ; in the latter case, let  $\omega(f) = r$ . The function  $\omega(f)$  has clearly the property

$$A. \quad \omega(f+g) \geq \min(\omega(f), \omega(g)).$$

Further we prove that it has the property

$$B. \quad \omega(f \cdot g) = \omega(f) + \omega(g).$$

*Proof.* If one of  $\omega(f)$  and  $\omega(g)$ , say  $\omega(f)$ , is  $\infty$ , then  $\sigma^n(f \cdot g) \equiv \sigma^n(f) \sigma^n(g) \equiv 0 \pmod{q_{n+1}}$  for all  $n$ . Hence  $\omega(f \cdot g) = \infty$ .

Suppose that both  $\omega(f)$  and  $\omega(g)$  are  $< \infty$ . According to the characteristic of  $P$  property B may be proved in two cases:

Case 1.  $p =$  the characteristic of  $P$ . By ii),  $\omega(f) = \omega(g) = 0$ , i.e.,  $f \not\equiv 0$  and  $g \not\equiv 0 \pmod{q_1}$ . Since  $P[U]/q_1$  is a field,  $f \cdot g \not\equiv 0 \pmod{q_1}$ . Hence  $\omega(f \cdot g) = 0$ .

Case 2.  $p \neq$  the characteristic of  $P$ . Then  $P$  is of characteristic 0. Let the sequences  $a_0, a_1, a_2, \dots$  and  $b_0, b_1, b_2, \dots$  be defined for  $f$  and  $g$  respectively as in iv). Write  $\omega(f) = r$  and  $\omega(g) = s$ . By the definition of the sequence  $a_0, a_1, a_2, \dots$ , we have from iii)  $a_n = 0$  for all  $n < r$  but  $a_r \neq 0$ . Similarly,  $b_n = 0$  for all  $n < s$  but  $b_s \neq 0$ . So, from

$$\sigma^{r+s}(f) \equiv \sigma^{r+s}(p^r \psi(a_r) + \dots + p^{r+s} \psi(a_{r+s})) \pmod{q_{r+s+1}}$$

and

$$\sigma^{r+s}(g) \equiv \sigma^{r+s}(p^s \psi(b_s) + \dots + p^{r+s} \psi(b_{r+s})) \pmod{q_{r+s+1}}$$

we have

$$\sigma^{r+s}(f \cdot g) \equiv \sigma^{r+s}(p^{r+s} \psi(a_r) \psi(b_s)) \equiv p^{r+s} \sigma^{r+s}(\psi(a_r) \psi(b_s)) \pmod{q_{r+s+1}}.$$

Since  $a_r b_s \neq 0$ , we have, by i) and iii),  $\sigma^{r+s}(f.g) \equiv p^{r+s} \psi(a_r b_s) \not\equiv 0 \pmod{\mathfrak{q}_{r+s+1}}$ , but  $\sigma^n(f.g) \equiv \sigma^{r+s}(f.g) \equiv p^{r+s} \psi(a_r b_s) \equiv 0 \pmod{\mathfrak{q}_{n+1}}$  for all  $n < r+s$ . Hence  $\omega(f.g) = r+s$ .

Let  $\mathfrak{H}$  be the set of all elements  $x$  of the ground ring  $P[U]$  satisfying  $\omega(x) = \infty$ . By property A,  $\mathfrak{H}$  forms an additive group. By property B,  $\mathfrak{H}$  forms an ideal in  $P[U]$ . The ideal  $\mathfrak{H}$  is called the *ground ideal* of the ground ring  $P[U]$ .

By the definition of  $\omega$ , any two elements  $f$  and  $g$  in the same residue class modulo  $\mathfrak{H}$  have the same value  $\omega(f) = \omega(g)$ . Let  $\bar{f}$  denote the residue class modulo  $\mathfrak{H}$  which contains  $f$ . We define  $\omega(\bar{f}) = \omega(f)$  for all elements  $\bar{f}$  of the quotient ring  $\mathfrak{J} = P[U]/\mathfrak{H}$ . It is clear that properties A and B induce in  $\mathfrak{J}$  the properties

$$\alpha) \quad \omega(\bar{f} + \bar{g}) \geq \min(\omega(\bar{f}), \omega(\bar{g})).$$

and

$$\beta) \quad \omega(\bar{f} \cdot \bar{g}) = \omega(\bar{f}) + \omega(\bar{g}).$$

Besides, we have

$$\gamma) \quad \omega(\bar{f}) = \infty \text{ if and only if } \bar{f} = 0.$$

$\mathfrak{J}$  is an integral domain because of properties  $\beta)$  and  $\gamma)$ . The function  $\omega$  is thus an exponential valuation on  $\mathfrak{J}$ . By property i),  $\sigma(f) - f$  belongs to  $\mathfrak{H}$  for all  $f$  of  $P[U]$ . So  $\sigma$  maps each residue class into itself, i.e.,  $\overline{\sigma(f)} = \bar{f}$  or  $\sigma$  induces the identity transformation in  $\mathfrak{J}$ .

Let  $\bar{\psi}(a)$  and  $\bar{a}_n$  denote respectively the images of  $\psi(a)$  and  $a_n$  under the natural homomorphism  $P[U] \sim \mathfrak{J}$ .

We see that every element  $\bar{f}$  of  $\bar{a}_n$  has  $\omega(\bar{f}) \geq n$ . Now we show the converse. Let  $\omega(\bar{f}) \geq n > 0$  for an  $\bar{f}$ . Then  $\omega(f) \geq n$  and it implies  $\sigma^{n-1}(f) \in \mathfrak{q}_n$ . Since  $\overline{\sigma^{n-1}(f)} = \bar{f}$ ,  $\bar{f}$  together with  $\sigma^{n-1}(f)$  belongs to  $\bar{a}_n$ . Hence  $\bar{a}_n$  consists of all elements  $\bar{f}$  with  $\omega(\bar{f}) \geq n$ .

Since every element  $f$  of  $P[U]$  outside  $\mathfrak{q}_1$  has  $\tau(f) \neq 0$  and  $\omega(f) = 0$ ,  $f$  does not belong to  $\mathfrak{H}$ . So  $\mathfrak{H} \subseteq \mathfrak{q}_1$ . Under the natural homomorphism  $P[U] \sim \mathfrak{J}$ , the residue class ring of  $\mathfrak{J}$  modulo  $\bar{a}_1$  is therefore isomorphic with that of  $P[U]$  modulo  $\mathfrak{q}_1$ . Hence  $\mathfrak{J}/\bar{a}_1$  is isomorphic with  $\mathfrak{K}$ , because by (15)

$$\bar{\psi}(a) + \bar{\psi}(b) \equiv \bar{\psi}(a+b) \pmod{\bar{q}_1}.$$

Let  $\bar{\mathfrak{F}}$  be the closure of  $\mathfrak{F}$  and  $Q(\bar{\mathfrak{F}})$  the quotient field of  $\bar{\mathfrak{F}}$ . Let the extension of  $\omega$  to  $Q(\bar{\mathfrak{F}})$  be denoted by the same symbol  $\omega$  and let  $\mathfrak{p}$  be the ideal of  $\bar{\mathfrak{F}}$  consisting of all elements  $x$  with  $\omega(x) \geq 1$ .

At first we see  $\mathfrak{F} \leq \bar{\mathfrak{F}}$ ,  $\bar{q}_1 \leq \mathfrak{p}$  and  $\mathfrak{F} \cap \mathfrak{p} = \bar{q}_1$ . Moreover, since every residue class modulo  $\mathfrak{p}$  in  $\bar{\mathfrak{F}}$  is represented by exactly one  $\psi(a)$ , the mapping, which maps each residue class containing  $\bar{\psi}(a)$  modulo  $\bar{q}_1$  in  $\mathfrak{F}$  to the residue class containing the same  $\bar{\psi}(a)$  modulo  $\mathfrak{p}$  in  $\bar{\mathfrak{F}}$ , is an isomorphism, which is called a congruent isomorphism of  $\mathfrak{F}/\bar{q}_1$  with  $\bar{\mathfrak{F}}/\mathfrak{p}$  according to Hasse's definition. (see 1))

The quotient field  $Q(\bar{\mathfrak{F}})$  falls into different types according to  $\chi(P) = \chi(\mathfrak{R})$  or not, where  $\chi$  denotes the characteristic of a field or an integral domain.

Case 1.  $\chi(P) = \chi(\mathfrak{R})$ . Then  $p=0$  in  $P[U]$ . By ii), every element  $f$  of  $\bar{q}_1$  has  $\omega(f) = \infty$ . So  $\bar{q}_1 = (0)$ . The valuation  $\omega$  is therefore the trivial valuation. We have  $\bar{\mathfrak{F}} = \mathfrak{F}$ . Moreover, already  $\mathfrak{F}$  is isomorphic with  $\mathfrak{R}$  because

$$\bar{\psi}(a) + \bar{\psi}(b) = \bar{\psi}(a+b).$$

Hence  $Q(\bar{\mathfrak{F}}) = \bar{\mathfrak{F}}$ . Consequently,  $Q(\bar{\mathfrak{F}}) = \mathfrak{F}$ .

Case 2.  $\chi(P) \neq \chi(\mathfrak{R})$ . Then  $P$  is the ring of rational integers. Let  $\alpha$  be any positive integer and write  $\alpha = tp^r$  with  $(t, p) = 1$ . Since  $t \not\equiv 0 \pmod{q_1}$ , by iii),  $\alpha \not\equiv 0 \pmod{q_{r+1}}$ . So  $\omega(\bar{\alpha}) = r$  and then  $\alpha \bar{1} = \bar{\alpha} \neq 0$ . Hence  $\bar{\mathfrak{F}}$  is of characteristic 0. Since no two distinct integers of  $P$  belong to the same residue class modulo  $\bar{\mathfrak{F}}$ ,  $P$  may be imbedded in  $\bar{\mathfrak{F}}$  in the way that every residue class modulo  $\bar{\mathfrak{F}}$  which contains a rational integer  $\alpha$  is still denoted by the  $\alpha$ . It is considerable that the rational prime  $p$  has the least value  $\omega(p) = 1$ . Moreover, we have

iv)' In the case  $\chi(P) \neq \chi(\mathbb{K})$ , for each element  $\bar{f}$  of  $\bar{\mathfrak{F}}$ , there exists a unique sequence  $a_0, a_1, a_2, \dots$  in  $\mathfrak{R}$  such that

$$\bar{f} \equiv \bar{\psi}(a_0) + p\bar{\psi}(a_1) + \dots + p^n\bar{\psi}(a_n) \pmod{\bar{q}_{n+1}}.$$

*Proof.* The existence of the sequence follows directly from iv). To

show the uniqueness. Let  $b_0, b_1, b_2, \dots$  in  $\mathfrak{R}$  be another sequence satisfying our conditions. Let us assume that  $a_r, b_r$  be the first distinct pair. Then we have  $p^r \bar{\psi}(a_r) \equiv p^r \bar{\psi}(b_r) \pmod{\bar{q}_{r+1}}$ . But  $\omega(\bar{\psi}(a_r) - \bar{\psi}(b_r)) = 0$  since  $a_r \neq b_r$ . So  $\omega(p^r \bar{\psi}(a_r) - p^r \bar{\psi}(b_r)) = r$ . It would be  $p^r(\bar{\psi}(a_r) - \bar{\psi}(b_r)) \not\equiv 0 \pmod{\bar{q}_{r+1}}$ . A contradiction.

As usual way, it follows from iv), that the closure  $\bar{\mathfrak{J}}$  consists of all series  $\sum_{i=0}^{\infty} \bar{\psi}(a_i) p^i, a_i \in \mathfrak{R}$  and that the ideal  $\mathfrak{p}$  consists of all series  $\sum_{i=1}^{\infty} \bar{\psi}(a_i) p^i, a_i \in \mathfrak{R}$ . So  $\mathfrak{p}$  is the principal ideal  $(p)$ . It implies by induction that every element  $x$  of  $\bar{\mathfrak{J}}$  with  $\omega(x) = n$  has the form  $x = \varepsilon p^n, \omega(\varepsilon) = 0, \varepsilon \in \bar{\mathfrak{J}}$ . Since  $\bar{\mathfrak{J}}/(p)$  is a field, every element  $\varepsilon$  of  $\bar{\mathfrak{J}}$  with  $\omega(\varepsilon) = 0$  has an inverse in  $\bar{\mathfrak{J}}$ . So every element  $\gamma$  of the quotient field  $Q(\bar{\mathfrak{J}})$  has the form  $\varepsilon p^v$  ( $v \geq 0$ ) with a unit  $\varepsilon$  of  $\bar{\mathfrak{J}}$ . Hence  $\omega(\gamma) \geq 0$  if and only if  $v \geq 0$ , i.e.,  $\gamma$  belongs to  $\bar{\mathfrak{J}}$ . The  $\bar{\mathfrak{J}}$  is the valuation ring in  $Q(\bar{\mathfrak{J}})$  and  $(p)$  is the prime ideal of  $\bar{\mathfrak{J}}$ . Hence  $Q(\bar{\mathfrak{J}})$  is a  $p$ -adic field, whose residue class field is congruently isomorphic with that of  $\mathfrak{J}$ , where  $p$ -adic fields are understood to be discrete-valued, complete fields of characteristic 0 which have the rational prime  $p$  as a prime element.

For both cases, the field  $\mathfrak{R}$  may be identified with the residue class field of  $Q(\bar{\mathfrak{J}})$  in the way that each element  $a$  of  $\mathfrak{R}$  is regarded as the residue class containing  $\bar{\psi}(a)$ . Since  $\bar{\psi}(a) + \bar{\psi}(b) = \bar{\psi}(a+b)$  in Case 1, under the mapping  $a \rightarrow \bar{\psi}(a), a \in \mathfrak{R}$ , the system (1) holds for images of all elements of  $\mathfrak{R}$ , i.e., the system

$$\bar{\psi}(a) = \sum_i \bar{\psi}(a_i)^p \bar{\psi}(b_i)$$

holds in the representative system  $\{\bar{\psi}(a)\}$  of  $\mathfrak{R}$ .

It is also true for Case 2. Since  $\overline{\sigma(f)} = \bar{f}, f \in P[U]$ , it suffices to show that  $\sigma(\psi(a)) = \sum_i \psi(a_i)^p \psi(b_i)$  holds for all  $a$  of  $\mathfrak{R}$ . When  $a=0$ ,  $e, 0 = \sum_i 0^p b_i$  and  $e = e^p e$  are fundamental relations in (1). By (6),  $\sigma(\psi(0)) = \sum_i \psi(0)^p \psi(b_i)$  and  $\sigma(\psi(e)) = \psi(e)^p \psi(e)$ . For any  $a \in \mathfrak{R} - \mathfrak{M}$  except for  $a=0, e$ , we have  $\psi(a) = u(a)$ . So  $\sigma(\psi(a)) = \sum_i \psi(a_i)^p \psi(b_i)$  by (10). For any

$a \in \bar{\mathfrak{M}}$ , we obtain the fundamental relation  $\psi(a) = \psi(c)^p \psi(d)$ ,  $d \in \mathfrak{M}^*$ , from (12) by putting  $b = e$ . By (11),  $\sigma(\psi(a)) = \psi(c)^p \psi(d)$ .

Any representative system  $\{\bar{a}\}$  of  $\mathfrak{R}$  is called a *regular representative system or regular system* of  $\mathfrak{R}$  with respect to a  $p$ -basis  $\mathfrak{M}$  if the system (1) holds for images of all elements of  $\mathfrak{R}$  under the mapping  $a \rightarrow \bar{a}$ ,  $a \in \mathfrak{R}$ .

**THEOREM 1.** *For a given field  $\mathfrak{R}$  of characteristic  $p > 0$ , the quotient ring  $\mathfrak{F}$  of the ground ring  $P[U]$  with respect to any  $p$ -basis  $\mathfrak{M}$  modulo its ground ideal  $\mathfrak{H}$  is an integral domain with a discrete valuation  $\omega$  and has  $\mathfrak{R}$  as its residue class ring. Moreover, in the case  $\chi(P) = \chi(\mathfrak{R})$ ,  $\omega$  is the trivial valuation of  $\mathfrak{F}$  and thus  $\mathfrak{F}$  forms a field isomorphic with  $\mathfrak{R}$ . In the case  $\chi(P) \neq \chi(\mathfrak{R})$ , the quotient field of the closure of  $\mathfrak{F}$  is a  $p$ -adic field, whose residue class field is congruently isomorphic with that of  $\mathfrak{F}$  and contains a regular representative system of  $\mathfrak{R}$  with respect to the same  $p$ -basis  $\mathfrak{M}$ .*

## II. STRUCTURE THEOREM

Conversely, we begin with a given discrete-valued, complete field  $\bar{K}$  with residue class field  $\bar{\mathfrak{R}}$  of characteristic  $p > 0$ . Let  $\omega'$  denote the exponential valuation of  $\bar{K}$ . Let  $\bar{\mathfrak{F}}$  denote the valuation ring of  $\bar{K}$  consisting of all elements  $x$  with  $\omega'(x) \geq 1$  and let  $(\pi)$  be the prime ideal of  $\bar{\mathfrak{F}}$ .

Let  $\mathfrak{R}$  be any subfield of  $\bar{\mathfrak{R}}$  and let  $\mathfrak{M}$  be a  $p$ -basis of  $\mathfrak{R}$ . Let  $P$  be the primitive ring contained in  $\bar{K}$ . The ground ring  $P[U]$  of  $\mathfrak{R}$  with respect to the  $p$ -basis  $\mathfrak{M}$  and its ground ideal  $\mathfrak{H}$  have been defined in Part I. We shall show that there exists in  $\bar{\mathfrak{F}}$  a regular representative system of  $\mathfrak{R}$  with respect to the  $p$ -basis  $\mathfrak{M}$ . An analytical isomorphism of the quotient ring  $\mathfrak{F} = P[U]/\mathfrak{H}$  into the valuation ring  $\bar{\mathfrak{F}}$  will then be constructed.

At first, we define a system of sequences  $\varphi_0(a), \varphi_1(a), \varphi_2(a), \dots$ ,  $a \in \mathfrak{R}$  by recursive formula as follows: Let

$$(19) \quad \varphi_0(0) = 0 \quad \text{and} \quad \varphi_0(e) = 1,$$

and from each residue class  $a \in \mathfrak{M} \cup (\mathfrak{R} - \mathfrak{M})$ ,  $a \neq 0, e$ , we take arbitrarily

an element as  $\varphi_0(a)$ , and put

$$(20) \quad \varphi_0(c) = \prod_i \varphi_0(c_i)^{e_i} \quad \text{for all } c = \prod_i c_i^{e_i} \in \overline{\mathfrak{M}}, c_i \in \mathfrak{M}.$$

It is admissible because of the property c) following lemma 1.

Let us assume that  $\varphi_{n-1}(a)$  is defined for all  $a \in \mathfrak{R}$ . For each element  $a \in \mathfrak{R}$  we make use of the fundamental relation  $a = \sum_i a_i^p b_i$  in (1) and define

$$(21) \quad \varphi_n(a) = \sum_i \varphi_{n-1}(a_i)^p \varphi_0(b_i).$$

Thus, the system of sequences is defined.

We say that every sequence satisfies the congruence

$$\varphi_n(a) \equiv \varphi_{n-1}(a) \pmod{(\pi)^n}$$

for all  $n$ . It is trivial for  $n=1$ . Suppose it true for  $n$ . From (21), we have  $\varphi_{n+1}(a) - \varphi_n(a) = \sum_i [\varphi_n(a_i)^p - \varphi_{n-1}(a_i)^p] \varphi_0(b_i)$ . By Lemma 2,  $\varphi_n(a_i)^p \equiv \varphi_{n-1}(a_i)^p \pmod{(\pi)^{n+1}}$  for all  $i$ . So  $\varphi_{n+1}(a) \equiv \varphi_n(a) \pmod{(\pi)^{n+1}}$ . Hence every sequence is convergent.

Let  $\varphi(a) = \lim_{n \rightarrow \infty} \varphi_n(a)$  for each  $a$  of  $\mathfrak{R}$ . Since (19),  $\varphi_n(0) = \varphi_0(0)$  and  $\varphi_n(e) = \varphi_0(e)$  for all  $n$ . So

$$(22) \quad \varphi(0) = \varphi_0(0) = 0 \quad \text{and} \quad \varphi(e) = \varphi_0(e) = 1.$$

When  $\mathfrak{M}$  is non-empty, every element  $b$  of  $\overline{\mathfrak{M}}$  may be written as  $b = c^p d$  with  $c \in \overline{\mathfrak{M}}$  and  $d \in \mathfrak{M}^*$ . Since  $b = c^p d$  is a fundamental relation in (1),  $\varphi_n(b) = \varphi_{n-1}(c)^p \varphi_0(d)$ . Suppose that  $\varphi_{n-1}(b) = \varphi_0(b)$  holds for all  $b$  of  $\overline{\mathfrak{M}}$ . Then, by (20),  $\varphi_n(b) = \varphi_0(c)^p \varphi_0(d) = \varphi_0(c^p d) = \varphi_0(b)$  for all  $b$  of  $\overline{\mathfrak{M}}$ . We see  $\varphi_1(b) = \varphi_0(c)^p \varphi_0(d) = \varphi_0(b)$  for all  $b$  of  $\overline{\mathfrak{M}}$ . Hence

$$(23) \quad \varphi(b) = \varphi_0(b) \quad \text{for all } b \in \overline{\mathfrak{M}}.$$

This together with (20) implies

$$(24) \quad \varphi(b) = \prod_i \varphi_0(c_i)^{e_i} \quad \text{for all } b = \prod_i c_i^{e_i} \in \overline{\mathfrak{M}}, c_i \in \mathfrak{M}.$$

Let  $n$  tend to infinity in both sides of (21). Since (22) and (23) we have

$$(25) \quad \varphi(a) = \sum_i \varphi(a_i)^p \varphi(b_i).$$

Hence the representative system  $\{\varphi(a)\}$  is a regular system of  $\mathfrak{R}$  with respect to the  $p$ -basis  $\mathfrak{M}$ .

Let  $f(u(x_1), \dots, u(x_m)) \in P[U]$  be any polynomial in  $u(x_1), \dots, u(x_m)$  with coefficients in  $P$ . Then the mapping  $\varrho: f \rightarrow \varrho(f) = f(\varphi(x_1), \dots, \varphi(x_m))$  is clearly a homomorphism of the ground ring  $P[U]$  into the valuation ring  $\mathfrak{F}$ .

By (6), (8), (22) and (24), we have

$$(26) \quad \varrho(\psi(a)) = \varphi(a).$$

By (25) and the definition of  $\sigma$ , we have

$$(27) \quad \varrho(\sigma(f)) = \varphi(f).$$

Let  $\tau'$  be the natural homomorphism of  $\mathfrak{F}$  onto  $\bar{\mathfrak{R}}$ , i.e.  $\tau'(x)$  denote the residue class modulo  $(\pi)$ , which contains  $x \in \mathfrak{F}$ . Since  $\tau'(\varphi(a)) = a$ , we have from (14)

$$(28) \quad \tau'(\varrho(f)) = \tau(f).$$

Let  $q'_n$  denote the image of  $q_n$  under the homomorphism  $\varrho$  ( $n=1, 2, 3, \dots$ ). Since  $\tau$  maps  $q_1$  into 0, by (28),  $\tau'$  maps  $q'_1$  into 0, i.e., every element  $S' \in q'_1$  has  $\omega'(S') \geq \omega'(\pi)$ . Now  $\omega'(p) \geq \omega'(\pi)$ . So  $\omega'(p^i S'^{p^{n-i}-1}) \geq \omega'(\pi^n)$  for  $S' \in q'_1$ ,  $i=0, 1, \dots, n-1$ . By the definition of  $q_n$ , we have

$$(29) \quad \omega'(S') \geq \omega'(\pi^n) \quad \text{for all } S' \in q'_n.$$

We shall take  $\omega'(p) = 1$  in case  $\bar{K}$  is of characteristic 0. We show that

$$(30) \quad \omega'(\varrho(f)) = \omega(f).$$

For, if  $\omega(f) = \infty$ , then  $\sigma^n(f)$  belongs to  $q_{n+1}$  for all  $n$ . By (27) and (29),  $\omega'(\varrho(f)) = \omega'(\varrho(\sigma^n(f))) \geq \omega'(\pi^{n+1})$  for all  $n$ , which implies  $\omega'(\varrho(f)) = \infty$ . Suppose  $\omega(f) < \infty$ . (30) may be proved in two cases:

Case 1.  $\chi(P) = \chi(\mathfrak{R})$ . Then  $\omega(f) = 0$ , i.e.,  $\tau(f) \neq 0$ . By (28),  $\tau'(\varrho(f)) \neq 0$ . So  $\omega'(\varrho(f)) = 0$ .

Case 2.  $\chi(P) \neq \chi(\mathfrak{R})$ . Let the sequence  $a_0, a_1, a_2, \dots$  in  $\mathfrak{R}$  be defined for  $f \in P[U]$  as in iv). Write  $\omega(f) = r$ . We have  $a_n = 0$  for all  $n < r$  but  $a_r \neq 0$ . We choose an integer  $m$  so large that  $\omega'(\pi^m) \geq \omega'(p^r)$ . (of course  $m \geq r$ .) By iv)  $\sigma^m(f) = \sigma^m(p^r \psi(a_r) + \dots + p^m \psi(a_m)) + S$  with  $S \in \mathfrak{q}_{m+1}$ . So  $\varrho(f) = p^r \varphi(a_r) + \dots + p^m \varphi(a_m) + \varrho(S)$  with  $\varrho(S) \in \mathfrak{q}'_{m+1}$ . Since  $\omega'(\varrho(S)) \geq \omega'(\pi^{m+1}) \geq \omega'(p^r)$  and  $\omega'(\varphi(a_r)) = 0$ ,  $\omega'(\varrho(f)) = \omega'(p^r) = r$ . Hence (30) is proved.

Equation (30) shows that the ground ideal  $\mathfrak{J}$  is the kernel of the homomorphism  $\varrho$ . Let  $\mathfrak{J}'$  be the minimal subring of  $\mathfrak{J}$ , which contains the regular system  $\{\varphi(a)\}$ . Then  $\mathfrak{J}'$  is the image of  $P[U]$  under the homomorphism  $\varrho$ . Let  $\bar{\varrho}$  denote the natural isomorphism of  $\mathfrak{J} = P[U]/\mathfrak{J}$  onto  $\mathfrak{J}'$ , i.e., the isomorphism induced by  $\varrho$ :  $\bar{\varrho}(\bar{f}) = \varrho(f)$ . By the definition of the valuation  $\omega$  of  $\mathfrak{J}$ , equation (30) implies

$$\omega'(\bar{\varrho}(\bar{f})) = \omega(\bar{f}).$$

Hence the isomorphism  $\varrho$  is analytical.

Thus we have

**THEOREM 2.** *If the residue class field  $\bar{\mathfrak{R}}$  of a discrete-valued, complete field  $\bar{K}$  is of characteristic  $p > 0$ , then, for each subfield  $\mathfrak{R}$  of  $\bar{\mathfrak{R}}$ , the valuation ring  $\bar{\mathfrak{J}}$  of  $\bar{K}$  contains a regular representative system  $\{\varphi(a)\}$  of  $\mathfrak{R}$  with respect to any  $p$ -basis  $\mathfrak{M}$  of  $\mathfrak{R}$ . Moreover, for each regular system  $\{\varphi(a)\}$  of  $\mathfrak{R}$  with respect to any  $p$ -basis  $\mathfrak{M}$ , the minimal subring of  $\bar{\mathfrak{J}}$  which contains the system  $\{\varphi(a)\}$  is analytically isomorphic to the quotient ring of the ground ring  $P[U]$  of  $\mathfrak{R}$  with respect to the same  $p$ -basis  $\mathfrak{M}$  modulo its ground ideal  $\mathfrak{J}$  in the way that each pair of representatives  $\varphi(a)$  and  $\bar{\psi}(a)$  of the same residue class  $a \in \mathfrak{R}$  are corresponded to each other, where  $\chi(P) = \chi(\bar{K})$ .*

Finally we observe that each regular system  $\{\varphi(a)\}$  of  $\mathfrak{R}$  with respect to a  $p$ -basis  $\mathfrak{M}$  has the preassigned values  $\varphi(a)$  for all  $a \in \mathfrak{M}$ , and is



uniquely determined by its representative system of  $\mathfrak{M}$ . In particular, if  $\mathfrak{R}$  is perfect, then  $\{\varphi(a)\}$  is unique and is the multiplicative representative system.

For, the first part follows directly from (23). any regular system  $\{\varphi(a)\}$  has  $\varphi(e)=1$  and  $\varphi(0)=0$ . For the relation  $\varphi(e)=\varphi(e)^{1+p}$  in (25) implies  $\varphi(e)=1$ , and this together with  $\varphi(0)=\varphi(0)^p \varphi(e)$  implies  $\varphi(0)=0$ . Now we show the second part. Let  $\{\varphi_1(a)\}$  and  $\{\varphi_2(a)\}$  be any two regular systems of  $\mathfrak{R}$  with respect to the same  $p$ -basis  $\mathfrak{B}$ , and let  $\varphi_1(a)=\varphi_2(a)$  for all  $a \in \mathfrak{M}$ . Then by (24)  $\varphi_1(a)=\varphi_2(a)$ ,  $a \in \mathfrak{M}$ . In addition, we have  $\varphi_1(a)=\varphi_2(a)$ ,  $a=0, e$ . From (25) we have

$$(31) \quad \varphi_1(a) - \varphi_2(a) = \sum_i (\varphi_1(a_i)^p - \varphi_2(a_i)^p) \varphi_1(b_i)$$

for all  $a$  of  $\mathfrak{R}$ . Already we have  $\omega'(\varphi_1(a) - \varphi_2(a)) \geq 1$ . Assume  $\omega'(\varphi_1(a) - \varphi_2(a)) \geq n$  ( $n \geq 1$ ). By Lemma 2, (31) implies  $\omega'(\varphi_1(a) - \varphi_2(a)) \geq n+1$ . Hence by induction  $\omega'(\varphi_1(a) - \varphi_2(a)) = \infty$ , i.e., for all  $a$  of  $\mathfrak{R}$ ,  $\varphi_1(a) = \varphi_2(a)$ . So  $\{\varphi_1(a)\} = \{\varphi_2(a)\}$ .

If  $\mathfrak{R}$  is perfect, then its  $p$ -basis is empty. In this case the regular system of  $\mathfrak{R}$  is unique and is the multiplicative representative system.

*Remark.* Our results remains true if the regular system are generalized as follows: For, at the beginning of Part I, instead of the linear basis  $\mathfrak{M}^*$  of  $\mathfrak{R}/\mathfrak{R}^p$ , we may consider the general set  $\mathfrak{M}_n^*$  for any given positive integer  $n$ , which consists of all products  $\prod_i c_i^{e_i}$ , where  $0 \leq e_i \leq p^n - 1$  and  $c_1, \dots, c_r$  are distinct elements of a  $p$ -basis  $\mathfrak{M}$ . Similar to  $\mathfrak{M}^*$ ,  $\mathfrak{M}_n^*$  forms a linear basis of  $\mathfrak{R}$  over the subfield  $\mathfrak{R}^{p^n}$  of all  $p^n$ -th powers of elements of  $\mathfrak{R}$ . So every element  $a$  of  $\mathfrak{R}$  may be uniquely written as a linear combination of elements  $b_i$  of  $\mathfrak{M}_n^*$  with coefficients in  $\mathfrak{R}^{p^n}$ :

$$a = \sum_i a_i^{p^n} b_i.$$

These expressions form the system of fundamental relations of  $\mathfrak{R}$  with respect to the  $p$ -basis  $\mathfrak{M}$  and the positive integer  $n$ . If we make use of the system instead of the system (1) to define our endomorphism  $\sigma$  and our regular systems in Part I and construct the regular system  $\{\varphi(\alpha)\}$  in Part II, then the same results will be obtained.

(Received July, 11, 1951)