J. Math. Kyoto Univ. (JMKYAZ)
45-3 (2005), 633–644

The structure of a complete valuation ring with an infinite residue field

By

Aiichi Yamasaki

Introduction

The author has tried a generalization of Eichler type strong approximation theorem from the number fields to the quotient fields of general Dedekind domains. The trials were successful for the algebraic function field over the real field ([4],[5]). But soon more generalization turned out to be extremely difficult ([6]). It seems to be desirable to reconsider the structure of adele rings not over the number fields, but in more general setting. But this is already difficult, and as a first step, the author considered the local case, namely complete valuation rings. The author found no literature on this topic in a general setting, and the study is based on the analogy to the case over the number fields ([2], [3]). The obtained result is the content of the present paper.

The above mentioned generalization of strong approximation theorem is important in the connection to the cancellation problems of modules over non-commutative orders, since the cancellation is affirmative if and only if the endomorphism ring has the strong approximation property ([1], [4]).

Let R be a complete valuation ring with some discrete valuation. The valuation is denoted additively by $v(x)$ and multiplicatively by $|x|$. Then for $x \in R$ we have $v(x) \in \mathbb{Z}$, $v(x) \geq 0$, and $|x| = a^{v(x)}$ for some $0 < a < 1$. (The choice of a does not affect the topology induced by $|\quad|$). Let P be the valuation ideal of R. It is the unique maximal ideal of R and R/P is a field k, called the residue field of R. When k is a finite field, the structures of the additive group R and the multiplicative group $1 + P$ are well known. They are explained for instance in [3] Chap. 2. In this paper, we investigate a generalization of these results to the case when k is an infinite field. We use the completion of the direct sum, which we shall explain first.

P is a principal ideal. Throughout this paper, we shall fix a generating element π of P and call it the primitive element. Then we have $P = \pi R$ and $v(\pi) = 1$. Also we have $P = \{x \in R | v(x) > 0\}$ and $R^\times = \{x \in R | v(x) = 0\}$.

Received May 12, 2005

1. The completion of the direct sum

Let $\{R_\lambda\}$ be an infinite family of complete valuation rings. The direct product $\prod_\lambda R_\lambda$ is given by $\prod_\lambda R_\lambda = \{(x_\lambda)|\forall\lambda,\, x_\lambda \in R_\lambda\}$, the addition and the multiplication being defined coordinatewize. The direct sum $\sum_\lambda R_\lambda$ is a subring of $\prod_\lambda R_\lambda$ defined by $\sum_\lambda R_\lambda = \{(x_\lambda) \in \prod_\lambda R_\lambda|\forall'\lambda,\, x_\lambda = 0\}$ where $\forall'\lambda,\, x_\lambda = 0$ means that $x_\lambda = 0$ except for finite number of λ.

For $x = (x_\lambda) \in \prod_\lambda R_\lambda$, consider the norm $|x| = \sup_\lambda |x_\lambda|$. (Since $\forall\lambda$, $|x_\lambda| \leq 1$, the supremum exists certainly. The supremum is actually the maximum, because the valuation is discrete). We consider the closure of $\sum_\lambda R_\lambda$ in the topology induced by $|\quad|$. Since each R_λ is complete, this closure is nothing but the completion. We shall call this closure the completion of the direct sum and denote it with $l_0^\infty(\{R_\lambda\})$.

$l_0^\infty(\{R_\lambda\})$ is a subring of $\prod_\lambda R_\lambda$, and is written as a set as follows:

$$l_0^\infty(\{R_\lambda\}) = \left\{(x_\lambda) \in \prod_\lambda R_\lambda | x_\lambda = 0 \text{ except for countable number of } \lambda \right.$$
$$\left. \text{and for each } \varepsilon > 0,\, |x_\lambda| < \varepsilon \text{ except for finite number of } \lambda \right\}.$$

2. The case of the characteristic zero

If the characteristic of R is $p > 0$, then the valuation is trivial on the prime field $\mathbb{F}_p$ so that $\mathbb{F}_p$ is contained in k, thus k has also the characteristic p.

If the characteristic of R is zero, then R contains the prime ring $\mathbb{Z}$. If the valuation is trivial on $\mathbb{Z}$, k contains $\mathbb{Z}$ so contains $\mathbb{Q}$, so that the characteristic of k is zero. If the valuation is not trivial on $\mathbb{Z}$, it is the p-adic valuation for some p, so $p \notin R^\times$ and $p \equiv 0 \mod P$. This implies that k contains $\mathbb{F}_p$, so the characteristic of k is p.

So three cases are possible. (1) Characteristics of R and k are both 0. (2) Characteristic of R is zero, but that of k is p. (3) Characteristics of R and k are both p. In this section, we shall investigate the case (1).

Assume that the characteristics of R and k are both 0. Then both R and k contains $\mathbb{Q}$ and the valuation is trivial on $\mathbb{Q}$. The primitive element π is transcendental over $\mathbb{Q}$ and R contains the ring of formal power series $\mathbb{Q}[[\pi]]$. So the additive group R becomes a $\mathbb{Q}[[\pi]]$-module.

Theorem 1. *The additive group R is isomorphic to the completion of the direct sum of many $\mathbb{Q}[[\pi]]$s as a $\mathbb{Q}[[\pi]]$-module. The multiplicative group $1 + P$ is also a $\mathbb{Q}[[\pi]]$-module and isomorphic to R as $\mathbb{Q}[[\pi]]$-modules. The isomorphism is given by the correspondence of the basis $R \ni v_\lambda \longleftrightarrow 1 + v_\lambda\pi \in 1 + P$.*

Proof. Since k contains $\mathbb{Q}$, k is a $\mathbb{Q}$-vector space. Let $\{\overline{v}_\lambda\}_{\lambda\in\Lambda}$ be a basis of k as a $\mathbb{Q}$-vector space. For each λ, let $v_\lambda \in R^\times$ be a representative of the coset $\overline{v}_\lambda \in k = R/P$. Then, all $\mathbb{Q}$-linear combinations of $\{v_\lambda\}$ form a complete

representative system of $k = R/P$. Similarly, all $\mathbb{Q}$-linear combinations of $\{v_\lambda \pi\}$ form a complete representative system of P/P^2, so on. This yields that all $\mathbb{Q}[[\pi]]$-linear combinations of $\{v_\lambda\}$ form a dense set in R.

For $x = \sum_\lambda \alpha_\lambda v_\lambda$, $\alpha_\lambda \in \mathbb{Q}[[\pi]]$, evidently we have

$$v(x) = \min_\lambda v(\alpha_\lambda) \tag{2.1}$$

or using the multiplicative valuation, we have

$$|x| = \sup_\lambda |\alpha_\lambda|. \tag{2.2}$$

This implies that the direct sum of $\{\mathbb{Q}[[\pi]]v_\lambda\}$ is homeomorphically imbedded in R. Taking the completion, we get

$$R \simeq l_0^\infty(\{\mathbb{Q}[[\pi]]v_\lambda\}) \quad \text{as a } \mathbb{Q}[[\pi]]\text{-module.} \tag{2.3}$$

Next, we shall consider the multiplicative group $1 + P$. For $x \in P$ and $r \in R$, $(1 + x)^r$ is defined by the power series

$$(1+x)^r = \sum_{j=0}^{\infty} \frac{r(r-1)\cdots(r-j+1)}{j!} x^j \tag{2.4}$$

which converges on $1+P$ since the valuation is trivial on $\mathbb{Q}$. Thus $1+P$ becomes an R-module, especially becomes a $\mathbb{Q}[[\pi]]$-module. Note that

$$(1+x)^r \in 1 + rx(1+P), \tag{2.5}$$

especially that

$$\prod_\lambda (1+v_\lambda\pi)^{\alpha_\lambda} \in 1 + \sum_\lambda \alpha_\lambda v_\lambda \pi (1+P), \quad \alpha_\lambda \in \mathbb{Q}[[\pi]]. \tag{2.6}$$

This implies that $\{1 + v_\lambda\pi\}$ generates a dense $\mathbb{Q}[[\pi]]$-module in $1 + P$ and $1 + x = \prod_\lambda (1 + v_\lambda\pi)^{\alpha_\lambda}$ yields

$$v(x) = \min_\lambda v(\alpha_\lambda) + 1 \tag{2.7}$$

or using the multiplicative valuation, we have

$$|x| = a \sup_\lambda |\alpha_\lambda| \quad (\text{with } |x| = a^{v(x)}). \tag{2.8}$$

This means that the direct sum of $\{(1+v_\lambda\pi)^{\mathbb{Q}[[\pi]]}\}$ is homeomorphically imbedded in $1 + P$. Taking the completion, we get

$$1 + P \simeq l_0^\infty(\{(1+v_\lambda\pi)^{\mathbb{Q}[[\pi]]}\}) \text{ as a } \mathbb{Q}[[\pi]]\text{-module.} \tag{2.9}$$

The last statement of the theorem is now obvious. □

3. The case of Char R=0 but Char k=p

In this case R contains $\mathbb{Z}$ and the valuation is p-adic on $\mathbb{Z}$. So R contains the p-adic ring $\mathbb{Z}_p$ and the additive group R becomes a $\mathbb{Z}_p$-module.

Let $v(p) = l > 0$, then R is an extension of $\mathbb{Z}_p$ with the ramification index l. Let $v_p(\alpha)$ be the discrete valuation on $\mathbb{Z}_p$ then we have $v(\alpha) = lv_p(\alpha)$ for $\alpha \in \mathbb{Z}_p \subset R$.

Theorem 2. *The additive group R is isomorphic to the completion of the direct sum of many $\mathbb{Z}_p$s as a $\mathbb{Z}_p$-module. The multiplicative group $1 + P$ is also a $\mathbb{Z}_p$-module and written as*

$$1 + P = H \times K \tag{3.1}$$

where H is a sub-$\mathbb{Z}_p$-module isomorphic to R and K is a finite cyclic group consisting of all p-th power roots of 1 in $1 + P$. The isomorphism between R and H is given by the correspondence of the basis, which can be written explicitly when k is a finite field.

Proof. Since k contains $\mathbb{F}_p$, k is a $\mathbb{F}_p$-vector space. Let $\{\overline{v}_\lambda\}_{\lambda\in\Lambda}$ be a basis of k over $\mathbb{F}_p$, and let $v_\lambda \in R^\times$ be a representative of the coset $\overline{v}_\lambda \in k = R/P$. Then all linear combinations $\sum_\lambda n_\lambda v_\lambda$ with $n_\lambda \in \mathbb{Z}$, $0 \le n_\lambda \le p-1$ form a complete representative system of $k = R/P$. Similarly all linear combinations $\sum_\lambda n_\lambda v_\lambda p^j \pi^m$ form a complete representative system of P^{jl+m}/P^{jl+m+1}. This implies that $\{v_\lambda \pi^m\}$ with $\lambda \in \Lambda$ and $0 \le m \le l-1$ generates a dense $\mathbb{Z}_p$-module in R.

For $x = \sum_{\lambda,m} \alpha_{\lambda,m} v_\lambda \pi^m$, $\alpha_{\lambda,m} \in \mathbb{Z}_p$, evidently we have

$$v(x) = \min_{m,\lambda}(v_p(\alpha_{\lambda,m})l + m), \tag{3.2}$$

so that

$$\min_{m,\lambda} v_p(\alpha_{\lambda,m})l \le v(x) \le \min_{m,\lambda} v_p(\alpha_{\lambda,m})l + l - 1, \tag{3.3}$$

which is equivalent to

$$\sup_{m,\lambda} |\alpha_{\lambda,m}|^l a^{l-1} \le |x| \le \sup_{m,\lambda} |\alpha_{\lambda,m}|^l. \tag{3.4}$$

Therefore the direct sum of $\{\mathbb{Z}_p v_\lambda \pi^m\}$ is homeomorphically imbedded in R, so that taking the completion, we get

$$R \simeq l_0^\infty(\{\mathbb{Z}_p v_\lambda \pi^m\}_{\lambda\in\Lambda, 0\le m\le l-1}) \quad \text{as a } \mathbb{Z}_p\text{-module.} \tag{3.5}$$

The multiplicative group $1 + P$ is rather complicated. The discussion will be divided into some subcases.

If n is not a multiple of p,then we have

$$(1 + x)^n \in 1 + \overline{n}x(1 + P) \tag{3.6}$$

where $n \equiv \overline{n} \mod p$ and $1 \leq \overline{n} \leq p-1$.

On the other hand, we have $(1+x)^p = 1 + px + \frac{p(p-1)}{2}x^2 + \cdots + x^p$ with $v(px) = v(x) + l$ and $v(x^p) = pv(x)$. Therefore we get

$$\text{if } v(x) < \frac{l}{p-1}, \text{ then } v((1+x)^p - 1) = pv(x) \tag{3.7}$$

$$\text{and } (1+x)^p \in 1 + x^p(1+P).$$

$$\text{if } v(x) > \frac{l}{p-1}, \text{ then } v((1+x)^p - 1) = v(x) + l \tag{3.8}$$

$$\text{and } (1+x)^p \in 1 + px(1+P).$$

$$\text{if } v(x) = \frac{l}{p-1}, \text{ then } v((x+1)^p - 1) \geq \frac{pl}{p-1} \, (= v(x) + l = pv(x)) \tag{3.9}$$

but the equality may not hold for some x.

Especially, if $1+P$ has a p-th root of 1, then l must be a multiple of $p-1$, and the p-th root has a form $1+x$ with $v(x) = \frac{l}{p-1}$.

Anyway $(1+x)^{p^j}$ converges to 1 as $j \to \infty$ for any $x \in P$. Therefore for a fixed x, the mapping $\mathbb{Z} \ni n \mapsto (1+x)^n$ is continuous in the p-adic topology, so that $(1+x)^\alpha$ can be defined for $\alpha \in \mathbb{Z}_p$. Thus $1+P$ becomes a $\mathbb{Z}_p$-module.

(a) The case that $l < p-1$.

In this case, we have $(1+x)^p \in 1 + px(1+P)$ for any $x \in P$. This yields $(1+x)^{p^j} \in 1 + p^j x(1+P)$ for any $j \geq 1$, and eventually $(1+x)^\alpha \in 1 + \alpha x(1+P)$ for any $\alpha \in \mathbb{Z}_p$.

Thus $1 + x = \prod_{\lambda,m}(1 + v_\lambda \pi^m)^{\alpha_{\lambda,m}}$, $\alpha_{\lambda,m} \in \mathbb{Z}_p$ implies

$$x \in \sum_{\lambda,m} \alpha_{\lambda,m} v_\lambda \pi^m (1+P). \tag{3.10}$$

This situation is the same as the additive group R. So that we have the result:

$$1 + P \simeq l_0^\infty(\{(1 + v_\lambda \pi^m)^{\mathbb{Z}_p}\}_{\lambda \in \Lambda, 1 \leq m \leq l}) \tag{3.11}$$

Evidently we have $R \simeq 1 + P$ as $\mathbb{Z}_p$-modules. The isomorphism is given by the correspondence of the basis $R \ni v_\lambda \pi^m \leftrightarrow 1 + v_\lambda \pi^{m+1} \in 1 + P$.

(b) The case that $l > p-1$ but l is not a multiple of $p-1$.

From (3.7) and (3.8), for $v(x) < \frac{l}{p-1}$, we have $(1+x)^p \in 1 + x^p(1+P)$ and

$$(1+x)^{p^j} \in 1 + p^{j-i} x^{p^i} (1+P) \tag{3.12}$$

where i is the smallest integer such that $p^i v(x) > \frac{l}{p-1}$. (But if $j < i$, then i in (3.12) should be replaced by j).

Thus we get

(3.13)
$$1+x=\prod_{\lambda}(1+v_\lambda\pi^m)^{n_\lambda p^j} \text{ implies } x\in\sum_{\lambda} n_\lambda p^{j-i(m)} v_\lambda^{p^{i(m)}}\pi^{mp^{i(m)}}(1+P)$$

where $i(m)$ is the smallest integer such that $p^i m > \frac{l}{p-1}$. Again in (3.13), $i(m)$ should be replaced by j if $j < i(m)$.

Especially (3.13) implies

$$v(x)=(j-i(m))l+mp^{i(m)}, \tag{3.14}$$

so when j runs over $0,1,2,\ldots,v(x)$ can be $m, mp,\ldots,mp^{i(m)}, mp^{i(m)}+l, mp^{i(m)}+2l,\ldots$.

Therefore, when m runs over the following set, every value of $v(x)$ can appear just once.

$$1\le m<\frac{pl}{p-1},\ m \text{ is not a multiple of } p. \tag{3.15}$$

Case (b_1) The residue field k has the characteristic p, so that $\overline{r}\mapsto\overline{r}^p$ is a field isomorphism on k. We shall assume that $k^p=k$ for a while. When k is a finite field, this assumption is satisfied.

Under this assumption, $\{\overline{v}_\lambda^p\}$ is a basis of k over $\mathbb{F}_p$. Similarly $\{\overline{v}_\lambda^{p^j}\}$ is a basis of k over $\mathbb{F}_p$ for any j. Now from (3.13), we see that when (n_λ) varies, $\prod_\lambda(1+v_\lambda\pi^m)^{n_\lambda p^j}$ supplies a complete representative system of P^n/P^{n+1} where $n=(j-i(m))l+mp^{i(m)}$. This enables us to show that $\{1+v_\lambda\pi^m\}_{\lambda,m}$ generates a dense $\mathbb{Z}_p$-module in $1+P$. (m runs over the set defined by (3.15)).

Now, suppose that $1+x=\prod_{\lambda,m}(1+v_\lambda\pi^m)^{\alpha_{\lambda,m}}$, $\alpha_{\lambda,m}\in\mathbb{Z}_p$, then from (3.14) we have

$$v(x)=\min_{\lambda,m}((v_p(\alpha_{\lambda,m})-i(m))l+mp^{i(m)}). \tag{3.16}$$

Let j_0 be the smallest integer such that $p^{j_0}>\frac{l}{p-1}$. Then we have $i(m)\le j_0$ and $mp^{i(m)}<\frac{pl}{p-1}$. Thus we get

$$\min_{\lambda,m} v_p(\alpha_{\lambda,m})l-j_0 l\le v(x)\le\min_{\lambda,m} v_p(\alpha_{\lambda,m})l+\frac{pl}{p-1}. \tag{3.17}$$

or in other words

$$\sup_{\lambda,m}|\alpha_{\lambda,m}|^l a^{\frac{pl}{p-1}}\le|x|\le\sup_{\lambda,m}|\alpha_{\lambda,m}|^l a^{-j_0 l}. \tag{3.18}$$

Thus the direct sum of $\{(1+v_\lambda\pi^m)^{\mathbb{Z}_p}\}$ is homeomorphically imbedded in $1+P$, so we get

$$1+P\simeq l_0^\infty(\{(1+v_\lambda\pi^m)^{\mathbb{Z}_p}\}_{\lambda,m}). \tag{3.19}$$

This time again, we have $R \simeq 1+P$ as $\mathbb{Z}_p$-modules. This comes from the fact that the set of m satisfying (3.15) consists of just l elements. Let $l=(p-1)s+t$ with $1 \leq t \leq p-2$. Then $[\frac{pl}{p-1}] = ps+t$, and s multiples of p exist under this value. So that $\#(\{m\}) = ps+t-s = (p-1)s+t = l$. The isomorphism $R \simeq 1+P$ is given by the correspondence of the basis $R \ni v_\lambda \pi^i \leftrightarrow 1+v_\lambda \pi^{m_i} \in 1+P$ where m_i is the i-th smallest number satisfying (3.15).

Case (b_2) Now we assume that $k^p \neq k$. Let $\{\overline{u}_{\lambda'}\}_{\lambda' \in \Lambda'}$ be a basis of a co-space of k^p over $\mathbb{F}_p$. Then $\{\overline{u}_{\lambda'}\} \cup \{\overline{v}_\lambda^p\}$ is a basis of k over $\mathbb{F}_p$.

For $m' = mp < \frac{pl}{p-1}$, $(m,p)=1$, the lost representative system of $P^{m'}/P^{m'+1}$ is regained by adding the $\{1+u_{\lambda'}\pi^{m'}\}$ to the basis. Similarly for $m' = mp^j < \frac{pl}{p-1}$, $(m,p)=1$, we use the fact that $\{\overline{v}_\lambda^{p^j}\} \cup \{\overline{u}_{\lambda'}^{p^{j-1}}\} \cup \{\overline{u}_{\lambda'}^{p^{j-2}}\} \cup \cdots \cup \{\overline{u}_{\lambda'}\}$ is a basis of k over $\mathbb{F}_p$. As a result, if we add $\{1+u_{\lambda'}\pi^{m'}\}$ to the basis where

$$1 \leq m' < \frac{pl}{p-1},\ m' \text{ is a multiple of } p, \tag{3.20}$$

the lost denseness is regained. So we have

$$1+P \simeq l_0^\infty \left(\{(1+v_\lambda \pi^m)^{\mathbb{Z}_p}\}_{\lambda,m} \cup \{(1+u_{\lambda'}\pi^{m'})^{\mathbb{Z}_p}\}_{\lambda',m'} \right). \tag{3.21}$$

This time again, we have $R \simeq 1+P$ as $\mathbb{Z}_p$-modules. In this case, since k is an infinite field, the cardinality of the basis does not change even if we add $\{(1+u_{\lambda'}\pi^{m'})\}$ to the basis. (The correspondence between the basis is not so explicit. We rely only on the equality of the cardinality of the basis).

(c) The case that l is a multiple of $p-1$.

For some x with $v(x) = \frac{l}{p-1}$, it can happen that

$$(1+x)^p \notin 1+R^\times \pi^{\frac{pl}{p-1}}. \tag{3.22}$$

First we shall investigate the condition for (3.22). Let $x = \alpha \pi^{\frac{l}{p-1}}$ and $p = r_0 \pi^l$ with $\alpha, r_0 \in R^\times$, then (3.22) is equivalent to

$$r_0 \alpha + \alpha^p \in P \tag{3.23}$$

or in other words

$$\overline{r}_0 \overline{\alpha} + \overline{\alpha}^p = 0 \text{ in } k. \tag{3.24}$$

The mapping $k \ni \overline{r} \mapsto \varphi(\overline{r}) = \overline{r}_0 \overline{r} + \overline{r}^p$ is $\mathbb{F}_p$-linear on k.

Case (c_1) Assume that φ is injective. Then (3.22) never happens. This assures that $\{1+v_\lambda \pi^m\} \cup \{1+u_{\lambda'}\pi^{m'}\}$ stated in (b) generates a direct sum $\mathbb{Z}_p$-module. So we can apply the same argument with (b) except that we need some addition to the basis. Let $\{\overline{w}_{\lambda''}\}$ be a basis of a co-space of $\varphi(k)$ over $\mathbb{F}_p$. Then $\{\varphi(\overline{v}_\lambda)\} \cup$

$\{\overline{w}_{\lambda''}\}$ is a basis of k over $\mathbb{F}_p$. To get a complete representative system of $P^{m''}/P^{m''+1}$ with $m'' = \frac{pl}{p-1}$, we need to add $\{1 + w_{\lambda''}\pi^{m''}\}$ to the basis. In other respects, the argument is the same as (b) and we get

$$1 + P \simeq l_0^\infty(\{(1 + y_\nu)^{\mathbb{Z}_p}\}) \text{ as a } \mathbb{Z}_p\text{-module} \tag{3.25}$$

where

$$\{y_\nu\} = \{v_\lambda \pi^m\} \cup \{u_{\lambda'}\pi^{m'}\} \cup \{w_{\lambda''}\pi^{m''}\}. \tag{3.26}$$

Here m and m' runs through the conditions (3.15) and (3.20), and $m'' = \frac{pl}{p-1}$. This time again, we get $R \simeq 1 + P$ as $\mathbb{Z}_p$-modules. When k is a finite field, the injectivity of φ implies the surjectivity of φ and $\{w_{\lambda''}\}$ is empty.

Case (c_2) Assume that φ is not injective. Then the kernel of φ is one-dimensional over $\mathbb{F}_p$, because $\varphi(\overline{\alpha}) = 0$ with $\overline{\alpha} \neq 0$ implies $\overline{r}_0 + \overline{\alpha}^{p-1} = 0$, so that $\overline{\alpha}$ is a $(p-1)$-th root of $-\overline{r}_0$, and other $(p-1)$-th roots of $-\overline{r}_0$ are obtained as $\mathbb{F}_p^\times \overline{\alpha}$.

Let $\varphi(\overline{r}_1) = 0$, which is the same thing with that $\overline{r}_1$ is a $(p-1)$-th root of $-\overline{r}_0$. Now, we shall rearrange the basis $\{\overline{v}_\lambda\}$ or $\{\overline{u}_{\lambda'}\}$ as follows. If $\frac{l}{p-1}$ is not a multiple of p, we choose $\{\overline{v}_\lambda\}$ such that it includes $\overline{r}_1$ and set $\overline{v}_0 = \overline{r}_1$. If $\frac{l}{p-1}$ is a multiple of p and $\overline{r}_1 \notin k^p$, we choose $\{\overline{u}_{\lambda'}\}$ such that it includes $\overline{r}_1$ and set $\overline{u}_0 = \overline{r}_1$. If $\frac{l}{p-1}$ is a multiple of p and $\overline{r}_1 \in k^p$, then let $\overline{r}_2$ be the p-th root of $\overline{r}_1$. If $\frac{l}{p(p-1)}$ is not a multiple of p, then we set $\overline{v}_0 = \overline{r}_2$. If $\frac{l}{p(p-1)}$ is a multiple of p and $\overline{r}_2 \notin k^p$, then we set $\overline{u}_0 = \overline{r}_2$. If $\frac{l}{p(p-1)}$ is a multiple of p and $\overline{r}_2 \in k^p$, take $\overline{r}_3$ such that $\overline{r}_3^p = \overline{r}_2$. Repeating this procedure, we obtain y_0 in (3.26) such that

$$(1 + y_0)^{p^{h-1}} \in 1 + r_1 \pi^{\frac{l}{p-1}}(1 + P) \text{ for some } h \geq 1. \tag{3.27}$$

Then $(1 + y_0)^{p^h} \notin 1 + R^\times \pi^{\frac{pl}{p-1}}$ by the definition of $\overline{r}_1$.

The family $\{y_\nu\}$ in (3.26) generates a dense $\mathbb{Z}_p$-module in $1 + P$, but this time it is not a direct sum just because φ is not injective. If we omit y_0 from $\{y_\nu\}$, the family $\{y_\nu\}_{\nu \neq 0}$ generates a direct sum $\mathbb{Z}_p$-module because φ is injective on a co-space of $\overline{r}_1$. Let H be the completion of the direct sum, namely

$$H = l_0^\infty(\{(1 + y_\nu)^{\mathbb{Z}_p}\}_{\nu \neq 0}). \tag{3.28}$$

It is isomorphic with R as a $\mathbb{Z}_p$-module. (When k is a finite field, since the codimension of $\varphi(k)$ is one, $\{w_{\lambda''}\}$ consists of one element, and this compensates the omission of y_0).

Now $1 + P$ is generated by H and $1 + y_0$. Note that if $v(x) > \frac{l}{p-1}$, then $1 + x$ can be expressed without using $1 + y_0$. This shows that $(1 + y_0)^{p^h} \in H$ and since $(1 + y_0)^{p^{h-1}} \notin H$ is obvious, we have $(1 + P)/H \simeq \mathbb{Z}/p^h\mathbb{Z}$.

Case (c_{21}) If $(1+y_0)^{p^h}=1$, then the group generated by $1+y_0$ is isomorphic with $(1+P)/H$, so that we get

$$1+P=H\times<1+y_0>\simeq R\times\mathbb{Z}/p^h\mathbb{Z} \text{ as a } \mathbb{Z}_p\text{-module.} \tag{3.29}$$

Case (c_{22}) If $(1+y_0)^{p^h}\neq 1$, since it belongs to H, we have the expression

$$(1+y_0)^{p^h}=\prod_{\nu\neq 0}(1+y_\nu)^{\alpha_\nu},\ \alpha_\nu\in\mathbb{Z}_p. \tag{3.30}$$

Put $h'=\min_\nu v_p(\alpha_\nu)$. Since $v((1+y_0)^{p^h}-1)>\frac{pl}{p-1}$, and since $(1+x)\mapsto(1+x)^p$ is bijective from $1+P^i$ to $1+P^{i+l}$ for $i>\frac{l}{p-1}$, we have $(1+y_0)^{p^h}\in H^p$, so that every α_ν can be divided by p thus we get $h'\geq 1$.

Assume that $h'\geq h$. Then we have $(1+y_0)^{p^h}\in H^{p^h}$ so that $(1+y_0)^{p^h}=(1+x)^{p^h}$ for some $1+x\in H$. Here we have $v(x)>v(y_0)$, because $v((1+x)^p-1)=pv(x)$ or $v(x)+l$ without jumping as the case of $(1+y_0)^{p^{h-1}}$. Let $1+z=(1+y_0)(1+x)^{-1}$, then we have $z\in y_0(1+P)$. So replacing y_0 by z is only the change of a representative of the same coset of $k=R/P$. Taking z from the first, we have $(1+z)^{p^h}=1$ and the situation is reduced to Case (c_{21}).

Assume that $1\leq h'<h$. Take y_1 such that $v_p(\alpha_1)=h'$. The family $\{y_\nu\}_{\nu\neq 1}$ also generates a direct sum $\mathbb{Z}_p$-module, because $(1+y_0)^{p^h}$ and $(1+y_1)^{p^{h'}}$ can be replaced with each other modulo $l_0^\infty(\{(1+y_\nu)^{\mathbb{Z}_p}\}_{\nu\neq 0,1})$. Let H' be the completion of this direct sum.

$$H'=l_0^\infty(\{(1+y_\nu)^{\mathbb{Z}_p}\}_{\nu\neq 1}\}). \tag{3.31}$$

Again we have $H'\simeq R$ as $\mathbb{Z}_p$-modules. Then $1+P$ is generated by H' and $1+y_1$. We have

$$(1+y_1)^{p^{h'}}=\prod_{\nu\neq 1}(1+y_\nu)^{\beta_\nu},\quad v_p(\beta_0)=h,\ v_p(\beta_\nu)=v_p(\alpha_\nu)\geq h'. \tag{3.32}$$

(In (3.30), if $\alpha_1=\gamma p^{h'}$ with $\gamma\in\mathbb{Z}_p^\times$, then $\beta_0=\gamma^{-1}p^h$ and $\beta_\nu=-\gamma^{-1}\alpha_\nu$). So $(1+y_1)^{p^{h'}}\in H'^{p^{h'}}$, therefore

$$(1+y_1)^{p^{h'}}=(1+x)^{p^{h'}} \text{ for some } 1+x\in H'. \tag{3.33}$$

Put $1+z=(1+y_1)(1+x)^{-1}$. Then $1+P$ is generated by H' and $1+z$. (Replacing y_1 by z is only the change of the representative of the coset $(1+P)/H'$). Since $(1+z)^{p^{h'}}=1$, we get

$$1+P=H'\times<1+z>\simeq R\times\mathbb{Z}/p^{h'}\mathbb{Z}. \tag{3.34}$$

Since H' is torsion free, $1+P$ has no root of 1 other than $<1+z>$. This completes the proof of Theorem 2. □

Remark. In Theorem 2 the order p^h of K has a relation that l is a multiple of $p^{h-1}(p-1)$, as seen in the proof. So for a given l, h can not be so large.

4. The case of the characteristic p

Suppose that both R and k has the characteristic p. Then R contains the prime field $\mathbb{F}_p$ and the valuation is trivial on $\mathbb{F}_p$. Since the primitive element π is transcendental over $\mathbb{F}_p$, R contains the ring of formal power series $\mathbb{F}_p[[\pi]]$. So the additive group R becomes a $\mathbb{F}_p[[\pi]]$-module.

On the other hand, the multiplicative group $1+P$ is torsion free, so it can not be isomorphic to R.

Theorem 3. *The additive group R is isomorphic to the completion of the direct sum of many $\mathbb{F}_p[[\pi]]$s as a $\mathbb{F}_p[[\pi]]$-module. The multiplicative group $1+P$ is a $\mathbb{Z}_p$-module and isomorphic to a countable direct product of the completions of direct sums of many $\mathbb{Z}_p$s as a $\mathbb{Z}_p$-module.*

Proof. Let $\{\overline{v}_\lambda\}$ be a basis of k as a $\mathbb{F}_p$-vector space, and $v_\lambda \in R^\times$ be a representative of $\overline{v}_\lambda \in k = R/P$. Then all $\mathbb{F}_p$-linear combinations of $\{v_\lambda\}$ form a complete representative system of $k = R/P$. Similarly all $\mathbb{F}_p$-linear combinations of $\{v_\lambda \pi\}$ form a complete representative system of P/P^2, so on. This implies that $\{v_\lambda\}$ generates a dense $\mathbb{F}_p[[\pi]]$-module in R. The same argument with §2 leads to the conclusion

$$R \simeq l_0^\infty(\{\mathbb{F}_p[[\pi]]v_\lambda\}) \text{ as a } \mathbb{F}_p[[\pi]]\text{-module.} \tag{4.1}$$

Next, we shall investigate the multiplicative group $1+P$. If n is not a multiple of p, then

$$(1+x)^n \in 1+\overline{n}x(1+P) \text{ where } n \equiv \overline{n} \mod p \text{ and } 1 \le \overline{n} \le p-1. \tag{4.2}$$

On the other hand, we have

$$(1+x)^p = 1+x^p \tag{4.3}$$

since the characteristic is p. Repeating p-th powers, we get

$$(1+x)^{p^j} = 1+x^{p^j}. \tag{4.4}$$

This situation resembles to that of §3 as the limit of $l \to \infty$. Since for a fixed x, $\mathbb{Z} \ni n \mapsto (1+x)^n$ is continuous in the p-adic topology, $(1+x)^\alpha$ can be defined for $\alpha \in \mathbb{Z}_p$ and $1+P$ becomes a $\mathbb{Z}_p$-module.

Let $\{\overline{u}_{\lambda'}\}$ be a basis of a co-space of k^p over $\mathbb{F}_p$, then $\{\overline{v}_\lambda^p\} \cup \{\overline{u}_{\lambda'}\}$ is a basis of k over $\mathbb{F}_p$. The same argument with §3 shows that the family

$$\{(1+v_\lambda \pi^m)_{\lambda,m}\} \cup \{(1+u_{\lambda'}\pi^{m'})_{\lambda',m'}\} \tag{4.5}$$

generates a dense $\mathbb{Z}_p$-module in $1+P$, where
(4.6)
m runs through all non-multiples of p, m' runs through all multiples of p

Though the obtained $\mathbb{Z}_p$-module is a direct sum, the completion should be taken in a topology different from the usual completion of the direct sum.

Suppose that $1+x=\prod_{\lambda,m}(1+v_\lambda\pi^m)^{\alpha_{\lambda,m}}\prod_{\lambda',m'}(1+u_{\lambda'}\pi^{m'})^{\alpha_{\lambda',m'}}$ where $\alpha_{\lambda,m}$ and $\alpha_{\lambda',m'}\in\mathbb{Z}_p$. Then we have

$$v(x)=\min\left(mp^{v_p(\alpha_{\lambda,m})},m'p^{v_p(\alpha_{\lambda',m'})}\right) \tag{4.7}$$

If we take the multiplicative valuation on $\mathbb{Z}_p$ with the base $\frac{1}{p}$, $\left(\text{namely}|\alpha|=\left(\frac{1}{p}\right)^{v_p(\alpha)}\right)$, then (4.7) becomes

$$v(x)=\min\left(\frac{m}{|\alpha_{\lambda,m}|},\frac{m'}{|\alpha_{\lambda',m'}|}\right). \tag{4.8}$$

Let the multiplicative valuation on R be taken with the base a, then we have $v(x)=\log_a|x|$. The function $\frac{1}{\log_a t}$ is positive for small positive t, and tends monotonically to zero as $t\to 0$. Thus the topology defined by the scale $\frac{1}{\log_a|x|}$ is identical with that defined by the scale $|x|$, so the topology in question should be taken in the norm

$$\sup\left(\frac{|\alpha_{\lambda,m}|}{m},\frac{|\alpha_{\lambda',m'}|}{m'}\right). \tag{4.9}$$

The completion in this norm is the so-called weighted completion. We shall discuss it in general in the next section. Here we state the result as follows.

$$1+P\simeq\prod_m l_0^\infty\left(\{(1+v_\lambda\pi^m)^{\mathbb{Z}_p}\}_\lambda\right)\times\prod_{m'}l_0^\infty\left(\{(1+u_{\lambda'}\pi^{m'})^{\mathbb{Z}_p}\}_{\lambda'}\right). \tag{4.10}$$

The proof will be given in the next section. □

5. The weighted completion of the direct sum

Let $\{R_\lambda\}$ be an infinite family of complete valuation rings. Suppose that a natural number n_λ is given for each λ. Consider a norm on $\prod_\lambda R_\lambda$ defined by

$$|x|=\sup_\lambda\frac{|x_\lambda|}{n_\lambda}\ \text{for}\ x=(x_\lambda). \tag{5.1}$$

The completion of $\sum_\lambda R_\lambda$ in this norm is called the weighted completion of the direct sum. If $\{n_\lambda\}$ is bounded, the weighted completion is identical with the usual completion without weight.

Theorem 4. *The weighted completion is isomorphic to*

$$\prod_{n=1}^{\infty} l_0^{\infty}(\{R_\lambda\}_{\lambda\in\Lambda_n}), \tag{5.2}$$

where

$$\Lambda_n = \{\lambda \in \Lambda \,|\, n_\lambda = n\}. \tag{5.3}$$

Proof. Since the direct product is the closure of the direct sum in the product topology, it suffices to show that the topology of the weighted completion is identical with the product topology of the topologies of the usual completions without weight. This can be shown as follows.

$\sup_\lambda \frac{|x_\lambda|}{n_\lambda} \le \varepsilon$ is equivalent to $\sup_{\lambda\in\Lambda_n} |x_\lambda| \le n\varepsilon$ for $\forall n$. Since $|x_\lambda| \le 1$ for any λ, the condition is meaningless for $n > \frac{1}{\varepsilon}$, so that it is equivalent to

$$\sup_{\lambda\in\Lambda_n} |x_\lambda| \le n\varepsilon \text{ for } 1 \le n \le \left[\frac{1}{\varepsilon}\right]. \tag{5.4}$$

Conversely, suppose that $\varepsilon_n > 0$ is given for $n = 1, 2, \ldots, N$. Then

$$\sup_\lambda \frac{|x_\lambda|}{n_\lambda} \le \min \frac{\varepsilon_n}{n} \text{ implies } \sup_{\lambda\in\Lambda_n} |x_\lambda| \le \varepsilon_n \text{ for } n = 1, 2, \ldots, N. \tag{5.5}$$

This shows that the topology of the weighted completion is identical with the product topology of the topologies of the usual completions without weight on each Λ_n. This leads to the result of Theorem 4. □

Department of Mathematics
Kyoto University
Kyoto, 606-8502, Japan
e-mail: yamasaki@math.kyoto-u.ac.jp

References

[1] H. Hijikata, *On the decomposition of lattices over orders*, J. Math. Soc. Japan **49**-3 (1997), 431–437.

[2] V. Platnonv and A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, 1994.

[3] A. Weil, *Basic Number Theory, Third edition*, Springer, 1974.

[4] A. Yamasaki, *Cancellation of lattices and approximation properties of division algebras*, J. Math. Kyoto Univ. **36**-4 (1996), 857–867.

[5] ———, *Strong approximation theorem for division algebras over* $\mathbb{R}(x)$, J. Math. Soc. Japan **49**-3 (1997), 455–467.

[6] ———, *Toward a generalization of strong approximation theorem to a general PF field*, J. Math. Kyoto Univ. **42**-3 (2002), 477–484.