66. A Valuational Interpretation of Kummer's Theory of Ideal Numbers

By Norio ADACHI
Department of Mathematics, Waseda University

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1985)

It is well-known that Kummer created "ideal complex numbers" in order to save the unique factorization into prime factors ([4], [3]). In modern terminology, they were the valuations in the cyclotomic field: *Ce que fait Kummer revient exactement, en langage moderne, à definir les valuations sur corps cyclotomiques* (Bourbaki [1], p. 122).

In the present paper, we shall show that Kummer's idea can be directly used to prove the fundamental theorem on the extension of valuations, in even simpler way than in usual proofs, if we invoke a conception of Dedekind presented in the supplements to the second edition of Dirichlet's *Vorlesungen über Zahlentheorie* [2].

We mean by a *valuation* a discrete normed exponential valuation. Let K be a field, v a valuation of K, A the valuation ring of v and π a uniformizer of v:

$$A=\{x(\in K)\,|\,v(x)\geqq 0\},\quad \text{and}\quad v(\pi)=1.$$

First lemma. *Notations being as above, let L be a finite (not necessarily separable) extension of the field K, and B the integral closure of A in L. Suppose that an element ψ of B have the two following properties:*

(1°) $\psi\equiv 0 \pmod{\pi}$,

(2°) *If for α and β of B we have $\alpha\beta\psi\equiv 0 \pmod{\pi}$, then we have $\alpha\psi\equiv 0 \pmod{\pi}$ or $\beta\psi\equiv 0 \pmod{\pi}$.*

Then there exists an extension of V of v to L such that $V(\pi)=V(\psi)+1$.

Here, and in what follows, $\alpha\equiv 0 \pmod{\pi}$ for $\alpha\in B$ means $\alpha\equiv 0 \pmod{\pi B}$, namely, $\alpha/\pi\in B$.

For the proof, we follow Edwards [3], which is extracted from Dedekind [2]. But we must treat also the case where the field L is inseparable over K. First we show that the ring B is completely integrally closed. Suppose that ξ be a non-zero element of B and α an element of L such that $\xi\alpha^n\in B$ for any non-negative integer n. There exists a positive integer q such that the set $L^q=\{x^q;\ x\in L\}$ is contained in the separable closure L_s of K in L. Then $\xi^q\alpha^{qn}\in B_s=\mathrm{L}_s\cap B$ for any non-negative n. The ring B_s is Noetherian, since the ring A is Noetherian and B_s is the integral closure of A in the separable extension L_s over K. Therefore B_s is completely integrally closed, since it is an integrally closed Noetherian ring. Hence $\alpha^q\in\beta_s\subseteq B$. This implies $\alpha\in B$, since B is integrally closed. Thus, as $\psi/\pi\notin B$, we have shown that for any non-zero element ξ of B there exists

a non-negative integer n such that $\xi(\psi/\pi)^n \in B$ but $\xi(\psi/\pi)^{n+1} \notin B$. Next we show that such a number n is uniquely determined. In order to do this, it suffices to show that if $\xi\alpha^n \in B$, then $\xi\alpha^m \in B$ for any non-negative integer m ($\leqslant n$). In fact $(\xi\alpha^m)^n = \xi^{n-m}(\xi\alpha^n)^m \in B$. Hence $\xi\alpha^m \in B$, since B is integrally closed.

We designate this uniquely determined number n for ξ by $V(\xi)$. Particularly we put $V(0)=\infty$. We can extend the map V of the ring B to non-negative integers, augmented by ∞, to the map of the field L to the rational integers, augmented by ∞. The map V has the following properties, whose proof is routine:

$$V(\alpha\beta) = V(\alpha) + V(\beta),$$
$$V(\alpha+\beta) \geqslant \mathrm{Min}\{V(\alpha), V(\beta)\},$$

and

$$V(\pi) = V(\psi) + 1.$$

Remark that the requirement (2°) in the statement of the lemma is used to prove the first equality above. From the last equality above we have $V(\pi/\psi)=1$, which implies that the map V is surjective. This completes the proof.

If for an extension V of a valuation v in K to L there exists ψ which satisfies the requirements (1°) and (2°), we say that V is a *good* extension of the valuation v. This is a temporary term, since we shall soon find that all extensions are good.

We give a characterization of ψ with the properties (1°) and (2°) as follows:

Second lemma. *Notations being as in First lemma, suppose that ψ be an element of B. Denote the image of $B\psi$ by the natural mapping of B onto $\bar{B}=B/\pi B$ by $\overline{B\psi}$: $\overline{B\psi}=\{x\psi \bmod \pi B;\ x \in B\}$. Then ψ satisfies the requirements* (1°) *and* (2°) *in First lemma, if and only if the ideal $\overline{B\psi}$ is minimal in $\bar{B}$.*

Proof. Let $\bar{\mathfrak{m}}$ be a minimal ideal in $\bar{B}$. Then clearly $\bar{\mathfrak{m}}$ is a principal ideal. Hence there exists an element ψ of B such that $\bar{\mathfrak{m}}=\overline{B\psi}$. This ψ satisfies the requirements (1°) and (2°). In fact, let α and β be two elements of B, and assume that $\alpha\beta\psi \equiv 0 \pmod{\pi}$ and $\alpha\psi \not\equiv 0 \pmod{\pi}$. Put $\psi'=\alpha\psi$. Then we have $\{\bar{0}\} \subsetneqq \overline{B\psi'} \subseteqq \overline{B\psi}$. Since $\overline{B\psi}$ is minimal, we have $\overline{B\psi'}=\overline{B\psi}$. Hence there exists γ of B such that $\psi \equiv \gamma\psi' \pmod{\pi}$. Hence we have $\beta\psi \equiv \beta\gamma\psi' \equiv \gamma\alpha\beta\psi \equiv 0 \pmod{\pi}$.

Conversely, let ψ be an element of B which satisfies the requirements (1°) and (2°). Suppose that ψ' be an element of B such that $\overline{B\psi'} \subseteqq \overline{B\psi}$. Then there exists an element α of B such that $\psi' \equiv \alpha\psi \pmod{\pi}$. Consider the homomorphism f of $\overline{B\psi}$ onto $\overline{B\psi'}$ defined by $f(\overline{\xi\psi})=\overline{\xi\psi'}$. Since $\dim_{\bar{A}} \overline{B\psi} > \dim_{\bar{A}} \overline{B\psi'}$, where $\bar{A}=A/\pi A$, we have an element β of B such that $\overline{\beta\psi} \neq \bar{0}$ but $f(\overline{\beta\psi})=\bar{0}$. Then $\alpha\beta\psi \equiv 0 \pmod{\pi}$ but $\beta\psi \not\equiv 0 \pmod{\pi}$. From the assumption we get $\alpha\psi \equiv 0 \pmod{\pi}$. Therefore we have $\overline{B\psi'}=\{\bar{0}\}$. This proves that $\overline{B\psi}$ is a minimal ideal.

From the two lemmas above we find the following: Given an element α of B which is not divisible by π, there exists a good extension of v to L such that $V(\alpha)<V(\pi)$. In fact, take ψ such that the ideal $\overline{B\psi}$ is contained in $\overline{B\alpha}$ and minimal. The element ψ determines a desired valuation.

The following is the fundamental theorem about the extension of a valuation, which we prove by the use of the preceding lemmas:

Theorem. *Any valuation v of the field K can be extended to any finite extension L of K. If L has the degree n over K, the valuation v has at most n extensions to L. Moreover, if $V_1, \cdots, V_m$ denote all the extensions of v to L, and $B_1, \cdots, B_m$ their valuation rings, then we have*

$$B=\bigcap_{j=1}^{m} B_j,$$

where B is the integral closure of the valuation ring A of v in L.

Proof. We shall first prove that the valuation v has at least one and at most n good extensions in the field L, and that if $V_1, \cdots, V_m$ are all the good extensions of v in the field L, and $B_1, \cdots, B_m$ their valuation rings, then

$$B=\bigcap_{j=1}^{m} B_j.$$

Consider the vector space $\overline{B}=B/\pi B$ over the field $\overline{A}=A/\pi A$. Let $\{\bar{x}_j\}$ be a finite family of elements of $\overline{B}$ which are linearly independent over $\overline{A}$. If we had a non-trivial linear relation $\sum_j a_j x_j=0$ with a_j in K, we could suppose that all the a_j are in A, and furthermore, by dividing them by a suitable power of π, we could also suppose that they are not all divisible by π; thus, by reducing the relation $\sum_j a_j x_j=0$, we would get a non-trivial relation $\sum_j a_j x_j \equiv 0 \pmod{\pi}$, with a_j in A; this is a contradiction. Therefore the elements x_j are linearly independent over K. This implies that $\dim_{\overline{A}} \overline{B} \leqq n$. (The equality holds, if L is a separable extension over K, since B is a free A-module of rank n.) Therefore $\overline{B}$ has minimum condition on ideals, so $\overline{B}$ has at least one and at most n minimal ideals, since the sum of minimal ideals in $\overline{B}$ is a direct sum.

Next suppose that $V_1, \cdots, V_m$, be all the good extensions of v in L, and that $B_1, \cdots, B_m$ be their valuation rings. Since it is obvious that $B \subseteq \bigcap_{j=1}^{m} B_j$, we have only to show the converse. Suppose $\alpha \notin B$. Since L is the quotient field of B, and a finite extension of K, we can write $\alpha=(\beta/a)$, $a \in A$, $\beta \in B$. If $v(a)=0$, then $\alpha \in B$, which contradicts the assumption. Hence $v(a)>0$. Therefore we may assume that β is not divisible by π. By the remark preceding the statement of the theorem, we can conclude that there is a good extension V_j of v such that $V_j(\alpha)<0$.

Now we shall show that any extension of v is good. Let V be any extension of v in L which is not good. The independence of valuations tells the existence of an element x of L such that $V_j(x)>0$ $(j=1, \cdots, m)$ and $V(x)<0$. From the first we have $x \in B$, while from the latter we have $x \notin B$, since any element which is integral over the valuation ring A in the

finite extension is contained in the valuation ring of any extension of the valuation. This is a contradiction, which completes the proof of the theorem. We have also the following corollary:

Corollary. *Any extension of a valuation of a field to a finite extension is a good valuation.*

References

[1] Bourbaki, N.: Eléments d'histoire des mathématiques. Masson, Paris (1984).
[2] Dedekind, R.: Supplements to *Vorlesungen über Zahlentheorie* by P.G.L. Dirichlet. 2nd ed., Braunschweig (1871).
[3] Edwards, H. M.: Genesis of ideal theory. Arch. Hist. Exact Sci., **23**, 321–378 (1980).
[4] Kummer, E. E.: Zur Theorie der complexen Zahlen. J. Reine Angew. Math., **35**, 319–326 (1847).