ON AN EXISTENCE LEMMA IN VALUATION THEORY

MASAYOSHI NAGATA, TADASI NAKAYAMA
AND TOSIRO TUZUKU

Recently one of the writers used,[1] in proving a theorem on the commutativity of certain division rings, the following lemma:

I. *Let L be a field and K be its proper subfield. Except either when L is of characteristic $p \neq 0$ and absolutely algebraic or when L is algebraic and purely inseparable over K, there exists a pair of distinct (special exponential) valuations in L which coincide on K.*

In fact there are infinitely many such pairs. More precise is the following theorem:

II. *Let K be a field which is either of characteristic 0 or not absolutely algebraic, and L be its separable finite extension. There exist then infinitely many valuations in L which are of 1st degree over K.*[2]

Naturally II includes the infiniteness of prime ideals of 1st degree in an algebraic number field (of finite degree). But the lemmas are perhaps not new. Indeed, II may be proved easily by modifying and generalizing Moriya's[3] elementary proof to the mentioned particular case. However, since the writers fail to find a literature where these facts are explicitly stated, it is perhaps without use to offer here a proof,[4] indeed a one which is still simpler than, though closely related, the one obtained in the mentioned way.

As I follows from II readily, we shall treat II only. Let $L = K(\alpha)$ and let

$$F(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

be the monic irreducible polynomial over K possessing α as a root; we consider the case $n > 1$ only. Let d be the discriminant of $F(x)$. It is sufficient to

Received March 31, 1953.

1) T. Nakayama, "On the commutativity of certain division rings," forthcoming in Canad. J. Math.

2) On considering the Galois field of L over K instead of L, it is then easy to show that there are infinitely many valuations in K each of which has $(L : K)$ distinct prolongations in L.

3) M. Moriya, "Rein arithmetischer Beweis über die Unendlichkeit der Primideale 1. Grades aus einem algebraeschen Zahlkörper," Jour. Fac. Sci. Hokkaido Univ. ser. I. vol. 9 (1950).

4) First the second writer gave a somewhat clumsy proof to I, for the purpose of using in his note 1), and then the first and the third writers gave simpler proofs, which the three writers cooperated in further simplifying and refining into the present one.

get infintely many pairs (w, ρ) of an element w in K and a valuation ρ in L with mutually (essentially) distinct ρ's such that for each pair (w, ρ)

$$\text{i) } \rho(d) = 0, \qquad \text{ii) } \rho(a_i) \geqq 0 \ (i = 1, 2, \ldots, n-1),$$
$$\text{iii) } \rho(\alpha - w) > 0.$$

For, with such a pair (w, ρ) and with

$$F(x + w) = x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$$

we have ($\rho(\alpha) \geqq 0$, $\rho(\omega) \geqq 0$ and)

$$\rho(b_0) = \rho(F(w)) = \rho(F(w)) - F(\alpha)) > 0,$$
$$\rho(b_1) = \rho(F'(w)) = 0, \quad \rho(b_i) \geqq 0 \qquad (i = 2, \ldots, n-i).$$

It follows from Hensel's lemma that $F(x+w)$ can be factorized in the ρ-completion of K into a product of form $G(x)x$ with $G(x)$ prime to x. This means that ρ is of degree 1 over K.

Now, our field K either has an element t transcendent over the prime field P or (is algebraic over the prime field P and) is of characteristic 0. In the former case we take a transcendency basis $(t, u_1, u_2, \ldots)$ of K over P, denote the algebraic closure of $P(u_1, u_2, \ldots)$ in K by Q, and set $Z = Q[t]$, $R = Q(t)$. In the latter case, on the other hand, we simply set $R = P$ and denote by Z the ring of rational integers which we consider as being contained in P. Let I be, in either case. the totality of elements in L integral over Z, and let $c \neq 0$ be an element of Z such that $c\alpha \in I$.[5] If we take an element ω_0 in Z which is of sufficiently high degree in t or of sufficiently large absolute value according as Z is $Q[t]$ or the ring of rational integers, then the norm for $R(\alpha)/R$ of $c\alpha - w_0$ is a non-unit in Z and there exists a prime ideal $\mathfrak{p}$ in $I \cap R(\alpha)$ containg $c\alpha - w_0$. Let ρ be a prolongation to L of the valuation of $R(\alpha)$ defined by $\mathfrak{p}$. We have $\rho(c\alpha - w_0) > 0$.

We want to get an infinity of w_0's such that the corresponding ρ's are all distinct. It is convenient, to do so, to choose our w_0, as is possible, so as $(c\alpha, w_0) = 1$ (in $I \cap R(\alpha)$); this implies, since $c\alpha - w_0 \in \mathfrak{p}$, that $c\alpha \notin \mathfrak{p}$ and $w_0 \notin \mathfrak{p}$. On supposing that we have chosen $w_0^{(1)}, w_0^{(2)}, \ldots, w_0^{(m)}$ and corresponding $\mathfrak{p}^{(1)}, \mathfrak{p}^{(2)}, \ldots, \mathfrak{p}^{(m)}$, satisfying the above condition as well as the last, so that $\mathfrak{p}^{(\nu)}$ are all distinct, we take $\omega_0^{(m+1)}$ satisfying our conditions from $\mathfrak{p}^{(1)}\mathfrak{p}^{(2)} \ldots \mathfrak{p}^{(m)} \cap Z$ (which is certainly possible). The corresponding prime ideal[6] is then different from $\mathfrak{p}^{(1)}, \mathfrak{p}^{(2)}, \ldots, \mathfrak{p}^{(m)}$, as $w_0^{(m+1)} \notin \mathfrak{p}^{(m+1)}$. We get thus an infinite sequence $\mathfrak{p}^{(1)}, \mathfrak{p}^{(2)}, \ldots$ of distinct prime ideals and correspondingly an infinite sequence $\rho^{(1)}$,

[5] We could without loss in generality start with an α contained in I, and then wording would be simplified a little in the sequel.

[6] We choose any one of the allowed ones.

https://doi.org/10.1017/S0027763000016986 Published online by Cambridge University Press

$\rho^{(2)}, \ldots$ of distinct valuations in L. It is clear that $\rho^{(\nu)}(d) = 0$, $\rho^{(\nu)}(a_i) \geqq 0$ (in fact $\rho^{(\nu)}(a_i) = 0$ whenever $a_i \neq 0$) and $\rho^{(\nu)}(c) = 0$ for almost all ν. For any of such ν's we have $\rho(\alpha - w) > 0$ with $w = w_0 c^{-1}$. Thus we have obtained an infinity of pairs (w, ρ), with distinct ρ's, satisfying i), ii), iii).

Mathematical Institute,
Nagoya University

https://doi.org/10.1017/S0027763000016986 Published online by Cambridge University Press