Zeitschrift: Commentarii Mathematici Helvetici

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 44 (1969)

Artikel: A Note on Purely Inseparable Extensions.

Autor: Ojanguren, M. / Sridharan, R.

DOI: https://doi.org/10.5169/seals-33788

A Note on Purely Inseparable Extensions

M. OJANGUREN and R. SRIDHARAN

Introduction

Let K be a field of characteristic $p>0$ and let L be a subfield of K such that K/L is a finite, purely inseparable extension of exponent 1. A Galois theory for such extensions using the concept of restricted Lie ring was initiated by Jacobson [4]. This theory gives a bijective correspondence between restricted Lie subrings of $\mathrm{Der}_L K$ (the Lie ring of all derivations of K vanishing on L) and subextensions of K/L. M. Gerstenhaber [1] showed that there is a bijection already between restricted subspaces of $\mathrm{Der}_L K$ and subextensions of K/L and as a consequence deduced that every restricted subspace of $\mathrm{Der}_L K$ is actually a Lie subring. In a subsequent paper [2], he generalized this Galois theory to the infinite case and showed that with the natural Krull-topology on $\mathrm{Der}\,K$, there is a bijective correspondence between closed restricted subspaces of $\mathrm{Der}\,K$ and subfields of K containing K^p. His proof, however, seems to be incomplete since Lemma 4 of [2] which is used to prove the theorem is incorrect.[1]) It is probable that this trouble may be circumvented and a suitably modified proof still holds. However, the aim of this note is to give another proof (Theorem 2) of the Galois correspondence, which, even in the finite dimensional case is different from the existing proofs in the literature (for example [3]). We also show (Theorem 1) that any restricted subspace of $\mathrm{Der}\,K$ (whether closed or not) is a Lie subring, by giving more or less an explicit formula for the commutator of two derivations.

In this paper, we use the notation and terminology of [2]. The authors have pleasure in thanking Prof. B. Eckmann for his keen interest in this work.

§ 1 Restricted Subspaces of $\mathrm{Der}\,K$

THEOREM 1. *Let K be a field of characteristic $p>0$ and V a restricted subspace of* $\mathrm{Der}\,K$. *Then V is a Lie subring.*

Proof: Let $\varphi, \psi \in V$. We wish to show that $[\varphi, \psi] \in V$. For this, we may clearly assume that $\varphi \neq 0$. Let $x \in K$ be such that $\varphi(x) \neq 0$. Since for any $k \in K$, $[k\varphi, \psi] = k[\varphi, \psi] - \psi(k)\varphi$, by taking $k = \varphi(x)^{-1}$, it is clear that we can assume $\varphi(x) = 1$.

For any $a \in \mathbf{Z}_p$ and any non negative integer m, we consider the element

[1]) That there is trouble with this Lemma was first noticed by H. Kubli. He now has another proof of the Galois correspondence which uses Theorem 1 of this note and the Galois theory for the finite case.

$\theta=(\varphi+ax^m\psi)^p$ in V. Expanding θ formally as a polynominal in a, we may write $\theta=\varphi^p+a\theta_1+\cdots+a^{p-1}\theta_{p-1}+a^p(x\psi)^p\in V$. Since φ^p and ψ^p are elements of V, we have the relation

$$\theta_1+a\theta_2+\cdots+a^{p-2}\theta_{p-1}\in V$$

for any non zero element a of $\mathbf{Z}_p$. Since the $(p-1)\times(p-1)$ Vandermonde matrix whose rows are $(1,a,\dots a^{p-2}), a\in\mathbf{Z}_p-(0)$, is non-singular, it follows from the above relations that $\theta_i\in V$ for $1\leqslant i\leqslant p-1$. In particular,

$$\theta_1=\theta_1(m,\psi)=\sum_{0\leqslant i\leqslant p-1}\varphi^i x^m\psi\varphi^{p-1-i}\in V$$

Using the fact that $\theta_1(m+1,\psi)=\theta_1(m,x\psi)$ and using induction on m, we get

$$\theta_1(m,\psi)=\sum_{0\leqslant k\leqslant m}\binom{m}{k}x^{m-k}\delta_k, \tag{*}$$

where

$$\delta_k=\sum_{0\leqslant h\leqslant p-1}k!\binom{p-h-1}{k}\varphi^{p-h-k-1}\psi\varphi^h.$$

Since $\delta_0=\theta_1(0,\psi)\in V$, it follows using (*) for $m=1,2,\dots$ that $\delta_k\in V$ for every k. In particular, $(p-1)!\,\varphi\psi+(p-2)!\,\psi\varphi=\delta_{p-2}\in V$ i.e. $\psi\varphi-\varphi\psi\in V$. This proves the theorem.[2])

§ 2 The Galois correspondence

Before proving the theorem on the Galois correspondence, we prove the following two lemmas.

LEMMA 1. *Let* $\theta_1,\dots\theta_r\in\operatorname{Der}K$ *and* $x\in K$ *such that all possible Lie brackets of all orders of* $\theta_1,\dots\theta_r$ *vanish on* x. *Then, for any permutation* σ *of* $(1,2,\dots r)$, *we have*

$$\theta_{\sigma(1)}\dots\theta_{\sigma(r)}(x)=\theta_1\dots\theta_r(x).$$

Proof: The lemma is clear for $r=2$. Let us assume that the lemma has been proved for $r-1$. We prove it for r, by showing that the result is true for all transpositions $(i,i+1)$, $1\leqslant i\leqslant r-1$. In fact we have

$$-\theta_1\dots\theta_{i+1}\theta_i\dots\theta_r(x)+\theta_1\dots\theta_i\theta_{i+1}\dots\theta_r(x)=\theta_1\dots[\theta_i,\theta_{i+1}]\dots\theta_r(x)$$

[2]) Added in proof: Prof. P. J. Higgins, who looked at this proof, has suggested another very elegant one.

Since the $r-1$ elements $\theta_1, \dots [\theta_i, \theta_{i+1}], \dots \theta_r$ clearly satisfy the condition of the lemma, the R.H.S. of the above equation is equal to $\theta_1 \dots \theta_r [\theta_i, \theta_{i+1}](x)=0$. This proves the lemma.

LEMMA 2. *Let V be a restricted subspace (hence, by Theorem 1, a Lie subring) of* Der$K$ *and let L be the field of constants of V. If $x_1, \dots x_n \in K$ are p-independent over L, then there exist $\varphi_1, \dots, \varphi_n \in V$ such that $\varphi_i(x_j)=\delta_{ij}$, $1 \leqslant i, j \leqslant n$.*

Proof: For $n=1$, the lemma is obvious. We assume that the lemma has been proved for n and prove it for $n+1$. Let then $x_1, \dots, x_{n+1} \in K$ be p-independent over L and let $\varphi_1 \in V$ be such that $\varphi_i(x_j)=\delta_{ij}$, $1 \leqslant i, j \leqslant n$. If there exists a $\psi \in V$ such that $\psi(x_i)=0$ for $1 \leqslant i \leqslant n$ and $\psi(x_{n+1}) \neq 0$, then the $n+1$ elements of V defined by

$$\varphi_i' = \varphi_i - \varphi_i(x_{n+1})\,\psi(x_{n+1})^{-1}\,\psi,\ 1 \leqslant i \leqslant n \quad \text{and} \quad \varphi_{n+1}' = \psi(x_{n+1})^{-1}\,\psi$$

satisfy the required properties and the lemma would be proved. Suppose then that for any $\psi \in V$ with $\psi(x_i)=0$ $1 \leqslant i \leqslant n$, we also have $\psi(x_{n+1})=0$. We now wish to contradict the p-independence of $x_1, \dots, x_{n+1}$ over L. Consider the element

$$c = \varphi_1^{p-1} \dots \varphi_n^{p-1}(x_{n+1}).$$

Since $\varphi_i(x_j)=\delta_{ij}$, $1 \leqslant i, j \leqslant n$, it follows that all the Lie brackets of all orders (which are in V since V is a Lie subring) vanish on x_k, $1 \leqslant k \leqslant n$ and therefore by our supposition on x_{n+1}. We may therefore apply Lemma 1 to $\varphi_1, \dots, \varphi_n \in V$ and $x_{n+1} \in K$ to get

$$\varphi_i(c) = \varphi_i \varphi_1^{p-1} \dots \varphi_n^{p-1}(x_{n+1}) = \varphi_1^{p-1} \dots \varphi_i^{p}(x_{n+1}) = 0,$$

since $\varphi_i^p \in V$ and $\varphi_i^p(x_j)=0$ for $1 \leqslant i \leqslant n$ and hence $\varphi_i^p(x_{n+1})=0$. If now $\psi \in V$ is such that $\psi(x_i)=0$ for $1 \leqslant i \leqslant n$, we clearly have $[\psi, \varphi_i](x_j)=0$ for $1 \leqslant i, j \leqslant n$ and since $[\psi, \varphi_i] \in V$, we have $[\psi, \varphi_i](x_{n+1})=0$, $1 \leqslant i \leqslant n$. We may again apply Lemma 1 to ψ, $\varphi_1, \dots, \varphi_n$ to conclude that

$$\psi(c) = \varphi_1^{p-1} \dots \varphi_n^{p-1}\,\psi(x_{n+1}) = 0,$$

since $\psi(x_i)=0$ for $1 \leqslant i \leqslant n$ and hence $\psi(x_{n+1})=0$. We now make a general remark which will also be needed later on in the proof: If $a \in K$ is such that $\varphi_i(a)=0$ for $1 \leqslant i \leqslant n$ and $\psi(a)=0$ for any $\psi \in V$ with $\psi(x_i)=0$ $1 \leqslant i \leqslant n$, then $\chi(a)=0$ for any $\chi \in V$. In fact we can write

$$\chi = \sum_{1 \leqslant i \leqslant n} \chi(x_i)\,\varphi_i + \psi,$$

$\psi \in V$ with the property $\psi(x_i)=0$ for $1 \leqslant i \leqslant n$. Hence

$$\chi(a) = \sum_{1 \leqslant i \leqslant n} \chi(x_i)\,\varphi_i(a) + \psi(a) = 0.$$

Applying this remark to c, we get that $c = \varphi_1^{p-1} \dots \varphi_n^{p-1}(x_{n+1}) \in L$.

We now show by descending induction that for any integer m with $0 \leqslant m \leqslant p-1$, there exists $Y_m \in L(x_1, \ldots x_n)$ with

$$\varphi_1^{\lambda_1} \ldots \varphi_n^{\lambda_n}(x_{n+1} - Y_m) = 0$$

for every n-tuple $(\lambda_1, \ldots \lambda_n)$ with $\sum \lambda_{i1} \geqslant m$ and $0 \leqslant \lambda_i \leqslant p-1$. To start the induction, we take $m = n(p-1)$ and

$$Y_{n(p-1)} = c \frac{x_1^{p-1} \ldots x_n^{p-1}}{((p-1)!)^n}.$$

Assume that Y_m has already been constructed. We proceed to construct Y_{m-1}.

For any n-tuple $(\lambda_1, \ldots \lambda_n)$ with $\sum \lambda_i = m-1$ and $0 \leqslant \lambda_i \leqslant p-1$, we define

$$\varphi_1^{\lambda_1} \ldots \varphi_n^{\lambda_n}(x_{n+1} - Y_m) = a_{\lambda_1 \ldots \lambda_n}.$$

We claim that $a_{\lambda_1 \ldots \lambda_n} \in L$. In fact,

$$\begin{aligned} \varphi_i(a_{\lambda_1 \ldots \lambda_n}) &= \varphi_i \varphi_1^{\lambda_1} \ldots \varphi_n^{\lambda_n}(x_{n+1} - Y_m) \\ &= \varphi_1^{\lambda_1} \ldots \varphi_i^{\lambda_i+1} \ldots \varphi_n^{\lambda_n} x_{n+1} - \varphi_1^{\lambda_1} \ldots \varphi_i^{\lambda_i+1} \ldots \varphi_n^{\lambda_n} Y_m \end{aligned}$$

by Lemma 1;

$$\begin{aligned} &= \varphi_1^{\lambda_1} \ldots \varphi_i^{\lambda_i+1} \ldots \varphi_n^{\lambda_n}(x_{n+1} - Y_m) \\ &= 0 \end{aligned}$$

by induction. Similarly, for any $\theta \in V$ with $\theta(x_i) = 0$ for $1 \leqslant i \leqslant n$, we have $\theta(a_{\lambda_1 \ldots \lambda_n}) = 0$. Hence, by our earlier remark, it follows that $a_{\lambda_1 \ldots \lambda_n} \in L$. Define

$$Y_{m-1} = Y_m + \sum_{\substack{\mu_1 + \cdots + \mu_n = m-1 \\ 0 \leqslant \mu_i \leqslant p-1}} \frac{a_{\mu_1 \ldots \mu_n}}{\mu_1! \ldots \mu_n!} x_1^{\mu_1} \ldots x_n^{\mu_n}.$$

We then have $\varphi_1^{\lambda_1} \ldots \varphi_n^{\lambda_n}(x_{n+1} - Y_{m-1}) = 0$ and this completes the induction. In particular, we have

$$x_{n+1} = \varphi_1^0 \ldots \varphi_n^0 (x_{n+1}) = Y_0 \in L(x_1, \ldots x_n).$$

This shows that $(x_1, \ldots x_{n+1})$ are p-dependent over L, a contradiction. This finishes the proof of Lemma 2.

We now prove the main

THEOREM 2. *Let K be a field of characteristic $p > 0$ and L a subfield of K containing K^p. The assignment $L \mapsto \mathrm{Der}_L K$ induces a bijection between the set of subfields of K containing K^p and the set of closed restricted subspaces of* Der K *(*Der K *being topologized by the usual Krull topology). The inverse correspondence is got by assigning to each closed restricted subspace of* Der K *its field of constants.*

Proof: For any subfield L of K containing K^p, clearly $\mathrm{Der}_L K$ is a closed subspace of $\mathrm{Der}\,K$ and it is well known that the field of constants of $\mathrm{Der}_L K$ is L. Let now V be a closed restricted subspace of $\mathrm{Der}\,K$ and let L be the field of constants of V. Clearly $V \subset \mathrm{Der}_L K$. We wish to show that $V = \mathrm{Der}_L K$. Since V is closed, it is enough to show that for any $x_1, \ldots, x_n \in K$ and $\varphi \in \mathrm{Der}_L K$, there exists a $\psi \in V$ such that $\psi(x_i) = \varphi(x_i)$ for $1 \leqslant i \leqslant n$. We may also assume without loss of generality that $x_1, \ldots, x_n$ are p-independent over L. By Lemma 2, there exist $\varphi_1, \ldots, \varphi_n \in V$ such that $\varphi_i(x_j) = \delta_{ij}$, $1 \leqslant i, j \leqslant n$. Then $\psi = \sum \varphi(x_i)\,\varphi_i \in V$ has the required property. This proves the theorem.

BIBLIOGRAPHY

[1] M. Gerstenhaber, *On the Galois theory of inseparable extensions*, Bull. Amer. Math. Soc. *70* (1964), 561–566.

[2] M. Gerstenhaber, *On infinite inseparable extensions of exponent one*, Bull. Amer. Math. Soc. *71* (1965), 878–881.

[3] G. Hochschild, *Simple algebras with purely inseparable splitting fields of exponent one*, Trans. Amer. Math. *79* (1955), 477–489.

[4] N. Jacobson, *Galois theory of purely inseparable fields of exponent one*, Amer. J. Math. *46* (1944), 645–648.

Forschungsinstitut für Mathematik, E.T.H. Zürich
Tata Institute of Fundamental Research, Bombay

Received October 20, 1968