ON MAXIMAL SUBFIELDS OF ENVELOPING SKEWFIELDS IN PRIME CHARACTERISTICS

JEAN-MARIE BOIS and GIL VERNIK

ABSTRACT. As was shown by Schue [6] there always exist two maximal subfields of the enveloping skewfields of a solvable Lie p-algebra, such that one is Galois and the second purely inseparable of exponent 1 over the centre. In this paper we obtain similar results for arbitrary solvable Lie algebras in prime characteristic, and for the Zassenhaus algebras. A key result here is to describe relations between maximal subfields in a polynomial extension of a division ring, and those of the base ring. We also provide a description of the enveloping algebra of the p-envelope of a Lie algebra as a polynomial extension of the smaller enveloping algebra.

INTRODUCTION

Let D be a division ring which is finitely generated over its centre Z, and let K be a subfield of D. The centralizer of K in D is defined by $C_D(K) = \{x \in D \mid [x, K] = 0\}$. The subfield K is called a *maximal subfield of* D if $C_D(K) = K$. Alternatively, a subfield $K \subseteq D$ containing Z is maximal if and only if $[D : K] = [K : Z] = \sqrt{[D : Z]}$ [2, thm. 4.2.2 and 4.3.2]. For more details about maximal subfields in the division rings one is referred to [2, 9].

A natural question is whether any central simple algebra affords a maximal subfield which is Galois over the centre (equivalently, whether such an algebra is a crossed product). The answer to this question is negative in general, see [9, Theorem 7.1.30]. In some special cases the answer may be positive. In [6], J. Schue showed that this is the case for the division ring of fractions of the enveloping algebra of a solvable Lie p-algebra over a field $\mathbb{F}$ of characteristic $p > 2$. In addition, in [6] was also shown the existence of a maximal subfield which is purely inseparable of exponent one over the centre.

The present paper is concerned with similar questions when L is any solvable Lie algebra over a field of prime characteristic. In particular a positive result is obtained for any solvable, not necessarily restrictable, Lie algebra of characteristic $p > 2$. Using a construction by Ermolaev [1], we also obtain a result for some simple Lie algebras, namely the Zassenhaus algebras.

The paper is organised as follows. In Section 1.1, we assume that D is a p-division algebra, ie. the dimension $[D : Z]$ is a power of $p = \mathrm{char}(Z)$. In that situation, we provide a link between the notions of tori in D, and Galois extensions of Z inside D whose Galois groups are p-elementary abelian (Theorem 1.1.4). In Section 1.2, we establish a reduction principle to construct maximal subfields in D from maximal subfields in a rational function field $D(u)$ (Proposition 1.2.4). As a corollary, we show that the structure of maximal commutative subfields can be transferred between D and $D(u)$ (Theorem 1.2.5).

Applications are given in Section 2. Let L be any solvable Lie algebra, or a Zassenhaus algebra (see 2.2.1 for the definition). It is proved that the enveloping skewfield of L in characteristic $p > 2$ contains maximal subfields which are Galois (resp. purely inseparable of exponent 1) over the centre (Theorems 2.1.7 and 2.2.2). A crucial ingredient for the proof in the solvable case is

Date: November 3, 2010.
2010 *Mathematics Subject Classification.* Primary 16K20, Secondary 17B35, 17B50.
Key words and phrases. Division ring, maximal subfield, Brauer group, enveloping algebra.
The first named author is supported by the D.F.G. priority programme SPP1388 "Darstellungstheorie". The second named author is supported by Minerva Fellowship Program.

the following. We prove that the enveloping field of a p-envelope of L is isomorphic to a ring of rational functions over the enveloping skewfield of L (Proposition 2.1.6). In view of the previous results, this allows us to reduce to the case of restrictable Lie algebras, which is known by results of J. Schue [6].

As a consequence of these theorems, we also show that the enveloping skewfield of L defines an element of order p in the Brauer group of its centre, when L is solvable and non-abelian, or $L = W(1, m)$. This suggests the following conjecture:

Conjecture. Let L be a non-abelian Lie algebra over a fields of characteristic $p > 2$, and let $K(L)$ be the enveloping skewfield. Then, $K(L)$ defines an element of order p in the Brauer group of its centre.

Acknowledgements. The authors wish to thank Rolf Farnsteiner for interesting comments on the results and suggestions of improvements.

1. A reduction principle for division rings

In what follows, we denote by $[V : D] := \dim_D(V)$ for a left vector space V over a division ring D. For an algebra A, we denote $Z(A)$ the centre of A. For a prime number p, we denote by $\mathbb{Z}_p$ the cyclic group with p elements and $\mathbb{F}_p$ the field with p elements; we use this notation to emphasise the field structure.

1.1. Preliminaries: tori in p-division algebras.

1.1.1. Before we deal with the reduction principle, we need some results on commutative subfields and tori in p-division algebras. Let D be a p-division algebra, that is to say, a division ring of characteristic $p > 0$, of dimension some power of p over its centre. We are interested in linking the notion of a torus in D with some class of subfields of D, which are Galois extensions of the centre Z. Recall that an element $t \in D$ is *toral* if $t^p - t \in Z$. Alternatively, this means that the inner derivation $\mathrm{ad}(t)$ is a toral element in the restricted Lie algebra $\mathrm{Der}_Z(D)$ [8, p. 79]. A *torus* is a commutative Z-subspace $T \subseteq D$ which is spanned by toral elements. In particular, $\mathrm{ad}(T)$ is a torus in $\mathrm{Der}_Z(L)$ [8, p.86]. We define the *rank of* T to be $[\mathrm{ad}(T) : Z]$.

Clearly, the unit element 1 is toral, and if T_0 is a torus, then $Z + T_0$ is a torus as well, of same rank. Since we are concerned with the adjoint action of tori on the division ring D, we will henceforth only consider tori containing 1.

1.1.2. We recall some standard facts related to actions of a torus. Let T be a torus, then there is a weight space decomposition

$$D = \bigoplus_{\lambda \in \Lambda} D_\lambda, \tag{1.1}$$

where $\Lambda \subseteq T^* = \mathrm{Hom}_Z(T, Z)$ is the *set of weights (of T in D)*. By definition,

$$D_\lambda = \{x \in D \mid (\forall\, t \in T),\ [t, x] = \lambda(t)x\},$$

and Λ is the set of linear forms λ such that $D_\lambda \neq (0)$. Note that $D_0 = C_D(T)$, the centralizer of T in D. It is easily seen that each D_λ is a D_0-vector space (on the left and on the right), of dimension 1. Furthermore, one readily checks that Λ is an additive subgroup of T^*, and the decomposition (1.1) is a Λ-grading of D.

1.1.3. The following result is essentially known [6, Section 2]. We give a different proof and a more precise statement.

Lemma. *Let D be a p-division algebra with centre Z. Let $T \subseteq D$ be a torus of rank d, and Λ be the corresponding set of weights. Then:*

(1) *The group $\Lambda \simeq \mathbb{Z}_p^d$.*

(2) *Let $Z(T) \subseteq D$ be the subfield generated by Z and T. Then $Z(T)$ is Galois over Z, and* $\mathrm{Gal}(Z(T)/Z) \simeq \Lambda$.

Proof. (1) We may assume that T contains 1. Let $\{t_0 \dots, t_d\}$ be a toral basis of T, with $t_0 = 1$. Let $T_p = \sum_{i=1}^d \mathbb{F}_p t_i$, and $\Lambda_p := \{\lambda|_{T_p} \mid \lambda \in \Lambda\} \subseteq \mathrm{Hom}_{\mathbb{F}_p}(T_p, Z)$. Since $t_0 = 1$ acts trivially on D, it is clear that $\Lambda \simeq \Lambda_p$. We will show that $\Lambda_p = T_p^* := \mathrm{Hom}_{\mathbb{F}_p}(T_p, \mathbb{F}_p)$, which will prove our first assertion.

First we show that $\Lambda_p \subseteq T_p^*$. For each $i \in \{1, \dots, d\}$, we have $(\mathrm{ad}\, t_i)^p - (\mathrm{ad}\, t_i) = 0$. Let $\lambda \in \Lambda$; since each $\lambda(t_i)$ is an eigenvalue of $\mathrm{ad}\, t_i$, we obtain $\lambda(t_i) \in \mathbb{F}_p$ as we wanted. For the reverse inclusion, we consider the natural non-degenerate pairing

$$\begin{array}{ccc} T_p \times T_p^* & \to & \mathbb{F}_p \\ (t, \lambda) & \mapsto & \lambda(t). \end{array}$$

Let $t \in \Lambda_p^\perp \subseteq T_p$. For all $\lambda \in \Lambda_p$ and all $x_\lambda \in D_\lambda$, we have $[t, x_\lambda] = \lambda(t)x_\lambda = 0$. Owing to (1.1), we obtain $[t, D] = 0$, so that $t \in Z \cap T_p$. Since $\{1, t_1, \dots, t_d\}$ is a Z-linearly independent family, we get $t = 0$. This proves $\Lambda_p^\perp = (0)$, hence $\Lambda_p = T_p^*$.

(2) For all $i \in \{1, \dots, d\}$, we have $t_i^p - t_i \in Z$, hence $[Z(T) : Z] \le p^d$. Furthermore, since each t_i is separable over Z, it follows that $Z(T)$ is separable over Z. In particular it admits a primitive element, say $\alpha \in Z(T)$.

Let $P(X) \in Z[X]$ be the minimal polynomial of α over Z, so that $\deg(P) = [Z(T) : Z]$. It is known that the cardinality $|\mathrm{Aut}_Z Z(T)|$ is the number of roots of $P(X)$ in $Z(T)$, whence $|\mathrm{Aut}_Z Z(T)| \le [Z(T) : Z]$. Thus, to show that $Z(T)$ is normal (and hence Galois) over Z it suffices to prove that $|\mathrm{Aut}_Z Z(T)| = [Z(T) : Z]$.

For all $\lambda \in \Lambda$, choose a non-zero element $x_\lambda \in D_\lambda$. For all $t \in T$, it is easily seen that $x_\lambda t x_\lambda^{-1} = t - \lambda(t)$, so that the inner automorphism defined by x_λ induces an automorphism $\sigma_\lambda \in \mathrm{Aut}_Z Z(T)$. One readily checks that the assignment $\lambda \in \Lambda \mapsto \sigma_\lambda \in \mathrm{Aut}_Z Z(T)$ is a group homomorphism. It is also injective, because $\sigma_\lambda = \mathrm{id}$ if and only if $t - \lambda(t) = \sigma_\lambda(t) = t$ for all $t \in T$. It follows $p^d \ge [Z(T) : Z] \ge |\mathrm{Aut}_Z Z(T)| \ge |\Lambda| = p^d$. Hence, equality holds everywhere. This shows that $Z(T)$ is Galois over Z, with $\mathrm{Gal}(Z(T)/Z) \simeq \Lambda$.

1.1.4. **Theorem.** *Let D be a finite-dimensional p-division algebra over its centre Z. Let $K \subseteq D$ be a commutative extension field of Z. The following are equivalent:*

- **(i)** *There exists a torus $T \subseteq K$ of rank d, such that $K = Z(T)$;*
- **(ii)** *K is a Galois extension of Z, and $\mathrm{Gal}(K/Z)$ is a p-elementary abelian group of rank d.*

Proof. **(i)** $\Rightarrow$ **(ii)** follows from Lemma 1.1.3, as well as the equality of ranks.

For **(ii)** $\Rightarrow$ **(i)**, assume that K is Galois over Z, with $\mathrm{Gal}(K/Z) \simeq \mathbb{Z}_p^d =: \Gamma$. For each $i \in \{1, \dots, d\}$, let $\Gamma_i = \mathbb{Z}_p \times \dots \times \{0\} \times \dots \times \mathbb{Z}_p$, where the trivial group occurs on the i-th slot. Set $K_i = K^{\Gamma_i}$. By [4, Cor. VI.1.16], we have $K = K_1 \cdots K_d$. Furthermore, each K_i is Galois over Z with Galois group $\Gamma/\Gamma_i \simeq \mathbb{Z}_p$. By the Theorem of Artin-Schreier [4, Th. VI.6.4], there exist $c_i \in Z, t_i \in K_i$ such that $K_i = Z(t_i)$ and $t_i^p - t_i - c_i = 0$. Then, $T = \sum_{i=1}^d Z t_i$ is a torus such that $K = Z(T)$.

1.1.5. We record a few more general results on tori in D.

Proposition. *Let D be a division p-algebra with centre Z. Let $[D : Z] = p^{2n}$, and let T be a torus of rank d. Recall the weight space decomposition $D = \bigoplus_{\lambda \in \Lambda} D_\lambda$. Then, the following are equivalent:*

- **(i)** *$n = d$;*
- **(ii)** *$Z(T)$ is a maximal subfield;*
- **(iii)** *D_0 is a maximal subfield;*
- **(iv)** *$D_0 = Z(T)$;*
- **(v)** *D_0 is commutative;*

(vi) $|\Lambda| = p^n$.

Proof. By Lemma 1.1.3, we have $|\Lambda| = p^d$, which proves **(i)** $\iff$ **(vi)**. The same lemma also gives $[Z(T) : Z] = p^d$. Recall that a commutative subfield $K \subseteq D$ containing Z is maximal if and only if $[K : Z] = p^n$, yielding **(i)** $\iff$ **(ii)**. Alternatively, such a field K is maximal commutative if and only if $C_D(K) = K$, if and only if $C_D(K)$ is commutative. Taking into account the fact that $C_D(Z(T)) = C_D(T) = D_0$, we readily obtain **(ii)** $\iff$ **(iv)** $\iff$ **(v)**. Finally, we have $C_D(D_0) \subseteq C_D(T) = D_0$. Hence, $C_D(D_0) = D_0$ if and only if D_0 is commutative, if and only if $C_D(D_0)$ is maximal commutative. This proves **(iii)** $\iff$ **(v)**.

1.2. **The reduction principle.**

1.2.1. In this section, we consider a finite-dimensional centra division algebra D over an infinite field Z. No restriction is made a priori on $\mathrm{char}(Z)$. We will say that a property *holds for almost all* $\lambda \in Z$ (or: *generically*) if the property holds for all except a finite number of values of λ.

1.2.2. *Rational functions over a division ring.* Consider the polynomial ring in several variables $Z[\underline{u}] = Z[u_1, \ldots, u_q]$, with field of fractions $Z(\underline{u}) = \mathrm{Frac}\, Z[\underline{u}]$. Consider $D[\underline{u}] := D \otimes_Z Z[\underline{u}]$, the polynomial ring in q variables over D. Note that $D[\underline{u}] \simeq D \otimes_{\mathbb{F}} \mathbb{F}[\underline{u}]$ for any central subfield $\mathbb{F} \subseteq Z$. We will identify D and $Z[\underline{u}]$ with the subalgebras $D \otimes_Z Z$ and $Z \otimes_Z Z[\underline{u}]$ of $D[\underline{u}]$. When $q = 1$, we use the symbol u instead of $\underline{u}$ or u_1. The following results are well-known:

Lemma.
(1) *The ring $D[\underline{u}]$ has a division ring of fractions, denoted $D(\underline{u})$.*
(2) *The centre of $D(\underline{u})$ is $Z(\underline{u})$, and $[D(\underline{u}) : Z(\underline{u})] = [D : Z]$. Further, $D(\underline{u}) \simeq D \otimes_Z Z(\underline{u})$.*
(3) *For all $\underline{\lambda} = (\lambda_1, \ldots, \lambda_q) \in Z^q$, there exists a unique algebra homomorphism $\pi_{\underline{\lambda}} : D[\underline{u}] \to D$ such that $\pi_{\underline{\lambda}}|_D = \mathrm{id}_D$ and $\pi_{\underline{\lambda}}(u_i) = \lambda_i$ for all $i \in \{1, \ldots, q\}$.*

1.2.3. For any subspace $V \subseteq D$ and $\lambda \in Z$, we define $\overline{V}_\lambda := \pi_\lambda(V \cap D[u]) \subseteq D$, which we call a *specialization of* V. If $V \supseteq Z(u)$, then $\overline{V}_\lambda \supseteq Z$. We will need the following simple lemma:

Lemma.
(1) *Let $\{a_1, \ldots, a_n\} \subseteq D[u]$ be $Z(u)$-linearly independent. Then, for almost all $\lambda \in Z$, the specializations $\{\pi_\lambda(a_1), \ldots, \pi_\lambda(a_n)\} \subseteq D$ are linearly independent over Z.*
(2) *Let $V \subseteq D(u)$ be a $Z(u)$-subspace of dimension n. Then, for almost all $\lambda \in Z$, the specialization $\overline{V}_\lambda$ is a Z-subspace of dimension n.*

Proof. (1) Let $\mathcal{B} = \{\beta_1, \ldots, \beta_N\}$ be a basis of D over Z, so that it is also a basis of $D[u]$ over $Z[u]$. Decompose each $a_i = \sum_{j=1}^N f_{ij}\, \beta_j$, with $f_{ij} = f_{ij}(u) \in Z[u]$. Let $A = [f_{ij}] \in M_{n,N}(Z[u])$. Since $\{a_1, \ldots, a_n\}$ is linearly independent over $Z(u)$, there is an $n \times n$ submatrix A_0 such that the minor $\det(A_0) \in Z[u] \smallsetminus \{0\}$.

Now note that for all i, $\pi_\lambda(a_i) = \sum_j \pi_\lambda(f_{ij})\beta_j$, so that the matrix $\pi_\lambda(A)$ represents the vectors $\{\pi_\lambda(a_1), \ldots, \pi_\lambda(a_n)\}$ in the basis $\mathcal{B}$. Then, the $n \times n$ minor $\det\big((\pi_\lambda(A_0)\big) = \pi_\lambda(\det A_0)$, which is non-zero for almost all values of λ. Hence, the matrix $\pi_\lambda(A)$ has full rank for almost all λ, in which case the family $\{\pi_\lambda(a_1), \ldots, \pi_\lambda(a_n)\}$ is linearly independent over Z.

(2) Let $\{a_1, \ldots, a_n\}$ be a $Z(u)$-basis of V. After multiplication by a suitable non-zero element of $Z[u]$, we may assume that all $a_i \in D[u]$. By (1), these elements almost always reduce to linearly independent elements in $\overline{V}_\lambda$, hence $[\overline{V}_\lambda : Z] \geq [V : Z(u)]$ for almost all $\lambda \in Z$. Conversely, let $\{b_1, \ldots, b_m\} \subseteq V \cap D[u]$ be a lifting of some Z-basis of $\overline{V}_\lambda$ and let $B \in M_{m,N}(Z[u])$ be the corresponding coefficients matrix. Since $\{\pi_\lambda(b_1), \ldots, \pi_\lambda(b_m)\}$ are linearly independent, as above there exists a non-vanishing $m \times m$ minor in the reduced matrix $\pi_\lambda(B)$. The corresponding minor of B is also nonzero, so that the matrix B has rank m over $Z(u)$. It readily follows $[\overline{V}_\lambda : Z] \leq [V : Z(u)]$.

1.2.4. Now we are ready to prove the reduction principle. We keep the previous notations.

Proposition. *Let $K \subseteq D(u)$ be an extension field of $Z(u)$, and $\lambda \in Z$.*

(1) *The specialization $\overline{K}_\lambda \subseteq D$ is an extension field of Z, and for almost all $\lambda \in Z$ we have $[\overline{K}_\lambda : Z] = [K : Z(u)]$. In particular, if K is a maximal commutative subfield of $D(u)$, then $\overline{K}_\lambda$ is generically a maximal subfield of D.*
(2) *If K is Galois over $Z(u)$, then K_λ is Galois over Z for almost all $\lambda \in Z$.*

If $\mathrm{char}(Z) = p > 0$, *we have in addition:*

(3) *If K is purely inseparable of exponent r over $Z(u)$, then $\overline{K}_\lambda$ is purely inseparable over Z, of exponent $\leq r$. Equality holds for almost all $\lambda \in Z$.*
(4) *If K is Galois over $Z(u)$, with Galois group $\mathbb{Z}_p^r$, then for almost all $\lambda \in Z$, $\overline{K}_\lambda$ is Galois over Z, with* $\mathrm{Gal}(\overline{K}_\lambda, Z) \simeq \mathbb{Z}_p^r$.

Proof. (1) By construction, $\overline{K}_\lambda$ is a finite-dimensional commutative domain over Z, so it is a field. Now, if $K \subseteq D(u)$ is a maximal subfield, then $[K : Z(u)]^2 = [D(u) : Z(u)]$. By Lemma 1.2.3, for almost all $\lambda \in Z$, we have $[\overline{K}_\lambda : Z]^2 = [K : Z(u)]^2 = [D : Z]$, and hence $\overline{K}_\lambda$ is a maximal subfield of D.

(2) Choose a primitive element $\alpha \in K$ over $Z(u)$. After multiplying by a suitable element of $Z[u]$ we may assume that $\alpha \in D[u]$. Let $P(X) = \sum_{i=1}^n c_i X^i \in Z(u)[X]$ be the minimal polynomial of α over $Z(u)$. Since K is Galois over $Z(u)$, this polynomial splits into linear factors $P(X) = \prod_{i=1}^n (X - \alpha_i)$, where each $\alpha_i \in K$. Now choose an element $c \in Z[u] \smallsetminus \{0\}$ such that $c\alpha_i \in D[u]$ for all i. Then α is a root of $c^n P(X) = \prod_{i=1}^n (cX - c\alpha_i) \in Z[u][X]$. For almost all $\lambda \in Z$, the element $\pi_\lambda(c) \neq 0$. Then $\pi_\lambda(\alpha)$ is a root of

$$P_\lambda(X) := \prod_{i=1}^n \big(X - \pi_\lambda(c)^{-1}\pi_\lambda(c\alpha_i)\big) \in Z[X].$$

Indeed, since $\alpha \in D[u]$ we can write $\pi_\lambda(c\alpha) = \pi_\lambda(c)\pi_\lambda(\alpha)$, and hence $(X - \alpha) \mid P_\lambda(X)$.

Now note that $\{c\alpha_1, \dots, c\alpha_n\}$ is a $Z(u)$-basis of K. By Lemma 1.2.3, $\{\pi_\lambda(c\alpha_1), \dots, \pi_\lambda(c\alpha_n)\}$ is a Z-basis of $\overline{K}_\lambda$ for almost all $\lambda \in Z$. It follows that $P_\lambda(X)$ is a separable polynomial, and also that $\overline{K}_\lambda = Z\big(\pi_\lambda(c\alpha_1), \dots, \pi_\lambda(c\alpha_n)\big)$ is the splitting field of $P_\lambda(X)$. This proves that $\overline{K}_\lambda$ is a Galois extension of Z.

(3) Let $x \in \overline{K}_\lambda$, and choose an element $a \in K \cap D[u]$ with $\pi_\lambda(a) = x$. Since K is purely inseparable of exponent r, we have $a^{p^r} \in Z[u]$, hence, $x^{p^r} = \pi_\lambda(a^{p^r}) \in Z$.

We check that the inseparability exponents coincide for almost all $\lambda \in Z$. There exists $a \in K$ such that $\{1, a, a^p \dots, a^{p^{r-1}}\}$ is linearly independent over $Z(u)$. We may assume that $a \in D[u]$. By Lemma 1.2.3, for almost all $\lambda \in Z$ the family $\{1, \pi_\lambda(a), \dots, \pi_\lambda(a)^{p^{r-1}}\}$ is linearly independent over Z: so the inseparability exponent of $\overline{K}_\lambda$ over Z is $> r - 1$.

(4) Recall that being Galois with a p-elementary abelian Galois group is equivalent to being generated by toral elements (Theorem 1.1.4). So we can write $K = Z(u)(t_1, \dots, t_n)$, where the t_i are toral and $\{1, t_1, \dots, t_n\}$ are $Z(u)$-linearly independent. It suffices to show that for almost all $\lambda \in Z$, there exist toral elements $\tau_1, \dots, \tau_n \in \overline{K}_\lambda$ such that $\{1, \tau_1, \dots, \tau_n\}$ are Z-linearly independent. Indeed, under these assumptions, we also know that $[K : Z(u)] = p^n = [Z(\tau_1, \dots, \tau_n) : Z]$, yielding $\overline{K}_\lambda = Z(\tau_1, \dots, \tau_n)$.

There exists $c \in Z[u] \smallsetminus \{0\}$ such that all $ct_i \in D[u]$. For almost all $\lambda \in Z$, the family $\{\pi_\lambda(c), \pi_\lambda(ct_1), \dots, \pi_\lambda(ct_n)\}$ is linearly independent over Z. In particular $\pi_\lambda(c) \neq 0$. A straightforward computation shows that each element $(ct_i)^p - c^{p-1}(ct_i)$ is central in $D[u]$. We obtain that each $\pi_\lambda(ct_i)^p - \pi_\lambda(c)^{p-1}\pi_\lambda(ct_i)$ is central, so that each $\tau_i := \pi_\lambda(c)^{-1}\pi_\lambda(ct_i)$ is toral in $\overline{K}_\lambda$. And by choice of λ, the family $\{1, \tau_1, \dots, \tau_n\}$ is Z-linearly independent.

1.2.5. *Transfer theorems.* Let D be a finite-dimensional division algebra over its centre Z, and $D(\underline{u})$ be a division ring of rational functions in several variables over D.

Theorem.

(1) *One has* $[D(\underline{u}) : Z(\underline{u})] = [D : Z]$, *and* $\operatorname{Exp} D(\underline{u}) = \operatorname{Exp} D$.
(2) $D(\underline{u})$ *has a maximal subfield which is Galois over* $Z(\underline{u})$ *if and only if* D *has a maximal subfield which is Galois over* Z.
(3) *When* $\operatorname{char}(Z) = p > 0$*:* $D(\underline{u})$ *has a maximal subfield which is purely inseparable of exponent* r *(resp. Galois with Galois group* $\mathbb{Z}_p^r$*) over* $Z(\underline{u})$ *if and only if* D *has a maximal subfield with the same property over* Z.

Proof. By induction it is enough to prove the theorem for a single variable, that is $q = 1$.

(1) The identity $[D(u) : Z(u)] = [D : Z]$ was proved in 1.2.2. For the exponent, recall that $D(u) \simeq D \otimes_Z Z(u)$ as algebras over $Z(u)$. For tensor powers, we compute:

$$\begin{aligned} D(u) \otimes_{Z(u)} D(u) &\simeq D \otimes_Z Z(u) \otimes_{Z(u)} Z(u) \otimes_Z D \\ &\simeq D \otimes_Z Z(u) \otimes_Z D \\ &\simeq D \otimes_Z D \otimes_Z Z(u). \end{aligned}$$

We obtain inductively that $D(u)^{\otimes n} \simeq D^{\otimes n} \otimes_Z Z(u)$, where the tensor power on the left is taken over $Z(u)$ and the one on the right over Z. If $D^{\otimes n}$ is trivial in the Brauer group $\operatorname{Br}(Z)$, then $D(u)^{\otimes n}$ is trivial in $\operatorname{Br} Z(u)$, so $\operatorname{Exp} D(u) \mid \operatorname{Exp}(D)$. Conversely, assume that $D^{\otimes n} \otimes_Z Z(u) \simeq M_q\big(Z(u)\big)$, for some $q \geq 1$. We know that $D^{\otimes n} \simeq M_N(\Delta)$, for some central division Z-algebra Δ and some integer $N \geq 1$; it follows $M_N(\Delta) \otimes_Z Z(u) \simeq M_q\big(Z(u)\big)$. Using the fact that $M_N(\Delta) \otimes_Z Z(u) \simeq M_N\big(\Delta(u)\big)$, we obtain an isomorphism

$$M_N\left(\Delta(u)\right) \simeq M_q\left(Z(u)\right).$$

This implies that $\Delta(u) \simeq Z(u)$. It follows that Δ is commutative, whence $\Delta = Z$. Thus, the algebra $D^{\otimes n}$ is trivial in the Brauer group $\operatorname{Br}(Z)$, and $\operatorname{Exp}(D) \mid \operatorname{Exp} D(u)$ as we wanted to show.

(2) and (3) The "only if" part follows from Proposition 1.2.4. Conversely, if D has a maximal subfield K satisfying any of the properties listed in (2) or (3), it is easy to check that $K \otimes_Z Z(u) \subseteq D(u)$ is a maximal subfield with the same property.

2. Applications

2.1. **Enveloping skewfields of non-restricted Lie algebras.**

2.1.1. In this section, $\mathbb{F}$ denotes an algebraically closed field of characteristic $p > 0$. Let L be a finite dimensional Lie algebra over $\mathbb{F}$. Let $U(L)$ be its enveloping algebra with centre $Z(L)$, and $K(L) = \operatorname{Frac} U(L)$ be the division ring of fractions of $U(L)$. We denote by $C(L)$ the centre of $K(L)$. The main result here is to show that when L is solvable, there always exists maximal subfields of $K(L)$ which are Galois or purely inseparable of exponent one over $C(L)$.

2.1.2. Recall that a Lie algebra is *restrictable* if there exists a map $x \in L \mapsto x^{[p]} \in L$, such that $(\operatorname{ad} x)^p = \operatorname{ad}(x^{[p]})$ for all $x \in L$. If L is restrictable, one can choose this map with some additional properties which mimick the properties of associative p-th powers in an associative algebra. In that case, the map is called a *p-mapping*, and L is called a *restricted Lie algebra*. We don't write down explicitly these properties here, as they are quite technical and irrelevant in our situation; see [8, Chap. 2] for a comprehensive account.

Finally, in the enveloping algebra of a restricted Lie algebra, the subalgebra

$$Z_p(L) := \mathbb{F}\langle x^p - x^{[p]} \mid x \in L \rangle \subseteq U(L)$$

is contained in the centre of $U(L)$, and called the *p-centre of* $U(L)$.

2.1.3. We briefly recall the notion of a p-envelope, see [8, Section 2.5] or [7, Section 1.1] for details. Let L be embedded in a restricted Lie algebra G. The *p-envelope of L in G*, denoted $L_{(p)}$, is the smallest restricted Lie subalgebra of G containing L. Note that the structure of $L_{(p)}$ depends on the initial embedding. For example, if $L \subseteq \mathfrak{gl}(n)$, then the corresponding p-envelope $L_{(p)}$ is finite-dimensional. On the other hand, consider the natural inclusion $L \subseteq U(L)$, then the associated p-envelope is infinite-dimensional.

In the sequel, we will slightly abuse terminology by referring to "a p-envelope" of a Lie algebra L. By this we will always mean the p-envelope of L in some unspecified larger finite-dimensional restricted Lie algebra. Since L is finite-dimensional, it always affords finite-dimensional p-envelopes [8, Prop 2.5.3].

2.1.4. As an example consider 4-dimensional non restricted Lie algebra L defined by $[x, y] = y$, $[x, z] = \alpha z$, $[x, t] = t + y$ and $[y, z] = [y, t] = [z, t] = 0$, where $\alpha \notin \mathbb{F}_p$. Then L is centreless, and the adjoint representation provides an embedding of L into the restricted Lie algebra $\mathrm{Der}_{\mathbb{F}}(L)$. Then the p-envelope $L_{(p)} \subseteq \mathrm{Der}_{\mathbb{F}}(L)$ is

$$L_{(p)} = \mathrm{ad}(L) + \mathbb{F}\,\mathrm{ad}(x)^p + \mathbb{F}\,\mathrm{ad}(x)^{p^2}.$$

Now identify each element $h \in L$ with $\mathrm{ad}(h) \in \mathrm{ad}(L) \subseteq L_{(p)}$, and set $u := \mathrm{ad}(x)^p$, $v := \mathrm{ad}(x)^{p^2}$. We can see that in $L_{(p)}$, we have the relations

$$[u, v] = 0,\ [u, x] = 0,\ [u, y] = y,\ [u, t] = t,\ [u, z] = \alpha^p z,$$

$$[v, x] = 0,\ [v, y] = y,\ [v, t] = t,\ [v, z] = \alpha^{p^2} z.$$

The other brackets are the ones coming from L. Here, one can check directly that L is an ideal in $L_{(p)}$. The following lemma provides a general description of how L embeds into $L_{(p)}$:

2.1.5. **Lemma.** *Let L be a finite dimensional Lie algebra over $\mathbb{F}$, and let $L_{(p)}$ be a finite-dimensional p-envelope of L. Then there exists a sequence $L_{(p)} = L_q \supseteq L_{q-1} \supseteq \cdots \supseteq L_0 = L$ such that, for all $i \in \{1, \ldots, q\}$:*

1. *$L_i = \mathbb{F}x_i + L_{i-1}$ for some $x_i \in L_i$,*
2. *there exists $y_i \in L_{i-1}$ with $y_{i-1}^{[p]} = x_i$,*
3. *each L_i is an ideal of $L_{(p)}$ such that $[L_{(p)}, L_i] = [L_0, L_0]$.*

Proof. We construct the L_i inductively. For $0 \leq i < q$, we have $L_i^{[p]} \not\subseteq L_i$, so there exists $y_i \in L_i$ such that $x_{i+1} := y_i^{[p]} \notin L_i$. Set $L_{i+1} := L_i \oplus \mathbb{F}x_{i+1}$. By construction these subspaces satisfy the first two conditions. Since each $L_i \supseteq L$, [8, Lemma 5.5] ensures that they are ideals of $L_{(p)}$. We show that $[L_i, L_0] = [L_0, L_0]$ for all $i \in \{0, \ldots, q\}$. For $i = 0$ there is nothing to show; now for $i > 0$ we have

$$\begin{aligned} [L_i, L_0] &= [L_{i-1}, L_0] + [x_i, L_0] \\ &= [L_{i-1}, L_0] + (\mathrm{ad}\, y_{i-1})^p(L_0) \\ &= [L_{i-1}, L_0] + [L_{i-1}, L_0] \\ &= [L_0, L_0], \end{aligned}$$

which is what we wanted.

2.1.6. The following result gives better description of the relation between $U(L)$ and $U(L_{(p)})$.

Proposition. *Let L be a finite dimensional Lie algebra over $\mathbb{F}$, and $L_{(p)}$ be a p-envelope. Then $U(L_{(p)}) \simeq U(L)[z_1, \ldots, z_q]$ with $q = \dim_{\mathbb{F}}(L_{(p)}/L)$. In particular, the enveloping field $K(L_{(p)}) \simeq D(L)(z_1, \ldots, z_q)$.*

Proof. Let $x_1, \ldots, x_q$, $y_0, \ldots, y_{q-1}$ be as in Lemma 2.1.5. Then, the elements $z_i := x_i - y_{i-1}^p$ are in the p-centre of $U(L_{(p)})$, hence commute with $U(L)$. Since $L_{(p)} = L \oplus \bigoplus_{i=1}^q \mathbb{F}x_i$, the

Poincaré-Birkhoff-Witt theorem implies that $U(L_{(p)}) = U(L)[z_1, \dots, z_q]$ is a polynomial ring in the variables $z_1, \dots, z_q$ over $U(L)$.

2.1.7. For a central simple algebra R over a field F, denote by $\mathrm{Exp}(R)$ the *exponent of* R, that is the order of R in the Brauer group of the centre [9, p. 214]. Alternatively, this is the smallest integer $n \geq 1$ such that the n-th tensor power $R^{\otimes n} \simeq M_N(F)$ for some integer N.

Theorem. *Assume that* $\mathrm{char}(\mathbb{F}) = p > 2$. *Let L be a finite-dimensional non-abelian solvable Lie algebra over $\mathbb{F}$. Then, the division ring $K(L)$ has the following properties:*

(1) *There exists a maximal subfield $F \subseteq K(L)$ which is Galois over the centre and the Galois group is p-elementary abelian;*
(2) *there exists a maximal subfield $E \subseteq K(L)$ which is purely inseparable, of exponent 1 over the centre;*
(3) $\mathrm{Exp}\, K(L) = p$.

Proof. By Proposition 2.1.6 and Theorem 1.2.5, it is enough to show the properties for restricted solvable algebras. Then (1) follow from [6, Theorem 3] and (2) follow from [6, Theorem 2]. Property (3) follows from (2) and [3, Th. 4.1.8].

2.1.8. As a consequence of Theorem 2.1.7, we obtain the following result. For a solvable Lie algebra in characteristic $p > 2$, there always exists a torus $T \subseteq K(L)$ which is "maximal" in the sense that $C_{K(L)}(T)$ is commutative. Alternatively, by Proposition 1.1.5, this means T has rank n, where $[K(L) : C(L)] = p^{2n}$. If L is restricted then it follows from Schue's results [6].

Corollary. *Assume that* $\mathrm{char}(\mathbb{F}) = p > 2$. *Let L be a finite dimensional solvable Lie algebra over $\mathbb{F}$. Then there exists a torus $T \subseteq K(L)$ such that $C_{K(L)}(T)$ is commutative.*

2.2. **The Zassenhaus algebra.**

2.2.1. Let $\mathbb{F}$ be algebraically closed of characteristic $p > 2$, and let $m \geq 1$ be a fixed integer. The *Zassenhaus algebra* is the simple Lie algebra of Cartan type $W(1, m)$ [7, Chap. 4.2]. Explicitly, $W(1, m)$ has a basis $\{e_{-1}, e_0, \dots, e_{p^m-2}\}$ with brackets:

$$[e_i, e_j] = \left(\binom{i+j+1}{i} - \binom{i+j+1}{j} \right) e_{i+j},$$

so $[e_i, e_j] = 0$ when $i + j \notin \{-1, \dots, p^m - 2\}$.

2.2.2. **Theorem.** *Let $\mathbb{F}$ be algebraically closed with* $\mathrm{char}(\mathbb{F}) > 2$. *Then, the enveloping skewfield $K\big(W(1, m)\big)$ has the following properties:*

(1) *There exists a maximal subfield which is Galois over the centre and the Galois group is p-elementary abelian;*
(2) *there exists a maximal subfield which is purely inseparable, of exponent 1 over the centre;*
(3) $\mathrm{Exp}\, K\big(W(1, m)\big) = p$.

Proof. For ease of notation, let $L := W(1, m)$. It is easy to see that the subspace $H := \sum_{i \geq 0} \mathbb{F}\, e_i$ is a solvable Lie subalgebra of codimension 1 in L. By Theorem 2.1.7, the properties of the theorem are satisfied in $K(H)$. By [1, Prop. 2], there exists a central element $z \in U(L)$ of the form $z = ae_{-1} + b$, where $a, b \in U(H)$, $a \neq 0$. Using the PBW theorem, we can see that z is transcendental over $U(H)$. Furthermore, it is clear that $K(L) = \mathrm{Frac}\, U(H)[z] = K(H)(z)$, so applying the transfer Theorem 1.2.5 yields the result.

References

[1] Y. Ermolaev: *Central elements of the universal enveloping algebra of the Zassenhaus algebra*, Izv. Vyssh. Uchebn. Zaved. Mat. 1978, no. 6 (193), 73–88.

[2] I.N. Herstein, "Noncommutative rings", The Carus Mathematical Monographs, Number Fifteen, Fourth printing, September 1996.

[3] N. Jacobson, "Finite-dimensional division algebras over fields", Springer-Verlag, Berlin, 1996.

[4] S. Lang, "Algebra", third edition, Reading, MA, Addison Wesley, 1993.

[5] J. Schue: *Structure theorems for the division ring associated with a solvable p-algebra*, Algebras Groups Geom. 9 (1992), no. 2, 81–98.

[6] J. Schue: *Enveloping algebras and division rings for Lie p-algebras*, Lie algebra and related topics (Madison, WI, 1988), 223230, Contemp. Math., 110, Amer. Math. Soc., Providence, RI, 1990.

[7] H. Strade, "Simple Lie algebras over fields of positive characteristic", Walter de Gruyter (2004).

[8] H. Strade and R. Farnsteiner, "Modular Lie algebras and their representations", Monographs and Textbooks in Pure and Applied Mathematics, 116. Marcel Dekker, Inc., New York, 1988.

[9] Louis H. Rowen, "Ring theory, Volume 2", Academic Press (1988).

Mathematisches Seminar, Christian-Albrechts-Universität zu Kiel, Ludewig-Meyn-Str. 4, 24098 Kiel, Germany

E-mail address: `bois@math.uni-kiel.de, vernik@math.uni-kiel.de`