A Galois theory of commutative rings

David J. Winter

University of Michigan, Ann Arbor, MI 48109-1109, USA

Received 23 July 2004
Available online 22 April 2005
Communicated by Michel Van den Bergh

Abstract


© 2005 Elsevier Inc. All rights reserved.

1. Introduction

This paper was inspired by ideas used in building infinite-dimensional simple Lie algebras [21] which led to a particularly simple proof of Jacobson’s differential correspondence theorem—written down in the foundations paper [19]. In turn, [19] and this proof inspired
the philosophy of this paper and the proof of its Theorem 4.2 as a generalization of Jacobson’s differential correspondence theorem from fields to commutative rings.

The unifying theme of [19]—using “dual bases” to prove Galois correspondence theorems—continues on as the unifying theme of this generalization of the Galois theory of fields to a Galois theory of commutative rings.

The most basic notion underlying this paper is that of a Galois correspondence [19] between sets $F$ and $G$ partially ordered by inclusion—a pair $(\text{op}, \text{po})$ of inclusion reversing maps $\text{op}: F \to G$, $F \leftarrow G : \text{po}$ such that

$$\text{po}(G) \supseteq F \iff G \subseteq \text{op}(F) \quad (F \in F, \ G \in G).$$

The notion of a Galois correspondence is quite general—and the condition for a Galois correspondence may be read as follows where the $F$ and $G$ are referred to, generally, as positions and operators:

**The position of $G$ contains the position $F$ if and only if the operator $G$ is contained in the operator of $F$.**

The roles of the positions (e.g., subfields considered below) and operators (e.g., groups, rings, Lie rings, birings considered below) are reversed in the dual Galois correspondence $(\text{op}, \text{po})$. The dual is a symmetry of the concept of Galois correspondence, so once general definitions and theorems are in place for positions (respectively operators), they apply to operators (respectively positions) by duality.

An element $F \in F$ (respectively $G \in G$) is **closed** when it equals its Galois correspondence closure $\bar{F} \equiv \text{po} \circ \text{op}(F)$ (respectively $\bar{G} \equiv \text{op} \circ \text{po}(G)$). Let $\tilde{F}$ (respectively $\tilde{G}$) denote the set of closed $F \in F$ (respectively closed $G \in G$)—and let $\overline{\text{op}}, \overline{\text{po}}$ denote the restrictions of $\text{op}$, $\text{po}$ to $\tilde{F}$, $\tilde{G}$, respectively. The functions $\overline{\text{op}}, \overline{\text{po}}$ are then inverses of each other. Consequently, $(\overline{\text{op}}, \overline{\text{po}})$—called the closed correspondence defined by $(\text{op}, \text{po})$—is a bijective Galois correspondence between $\tilde{F}$, $\tilde{G}$.

A Galois correspondence theorem is a theorem within some ambient Galois theory which establishes that some such $(\text{op}, \text{po})$ is a bijective Galois correspondence—or which describes some closed $F$’s and $G$’s of a Galois correspondence which correspond to each other. Such a Galois correspondence theorem is sometimes also referred to as a fundamental theorem of that ambient Galois theory.

The fundamental theorem of classical Galois theory establishes that the classical Galois correspondence $G \equiv \text{Aut}_F K$, $F \equiv K^G$ between the set $\text{FG}$ of subfields $F$ of a field $K$ such that $K$ is finite-dimensional Galois over $F$, that is, $K$ is the splitting field over $F$ of some separable polynomial, and the set $G$ of finite groups $G$ of automorphisms of $K$ is bijective. Here, $\text{Aut}_F K$ is the group of automorphisms of $K$ which fix the elements of $F$ and $K^G$ is the fixed field of $G$ on $K$.

Since a field $K$ has no ideals other than 0 and $K$, the following question arises:

*How does Galois theory generalize upon passage from a field $K$ to a commutative ring $A$ with respect to Galois objects acting irreducibly on $A$—without stable ideals other than 0 and $A$?*
This question is answered when the Galois objects are the Galois rings, groups, Lie rings, and birings of Sections 2–6. The fundamental theorems of the corresponding Galois rings, groups, Lie rings, and birings theories are then Theorems 2.1, 3.1, 4.2, 6.1, respectively.

1.1. Summary by sections

In Section 2, the Jacobson–Bourbaki Galois correspondence $F = KR$, $R = \text{End}_FK$ between the set $F_R$ of subfields $F$ of finite codimension of a field $K$ and the set $R$ of finite-dimensional endomorphism rings $R$ of $K$ [8,16,17] generalizes from fields $K$ to commutative rings $A$ in the Galois rings correspondence Theorem 2.1. It plays a supporting role in the Galois groups theory, Galois Lie rings theory, and Galois birings theory which follow.

In Section 3, the classical Galois correspondence generalizes from fields $K$ to commutative rings $A$ in the Galois groups correspondence Theorem 3.1.

In Section 4, the Jacobson differential Galois correspondence $D = \text{Der}_FK$, $F = K^D$ between the set $F_D$ of subfields $F$ of finite codimension of a field $K$ of prime characteristic $p$ such that $K^p \subseteq F$ and the set $D$ of finite-dimensional restricted derivation rings of $K$ [8,16] generalizes from fields $K$ to commutative rings $A$ in the Galois Lie rings correspondence Theorem 4.2.

In Section 5, derivation ring forms are introduced and studied. They lead to a more conceptual and self-contained proof of Theorem 4.2—as Corollary 5.1.

In Section 6, the Galois rings theory of Section 2 is transformed into a Galois biring theory by replacing the endomorphism rings $\text{End}_FA$ by their biring counterparts $\text{Pres}_FA = (\text{End}_FA, \Delta, \varepsilon)$.

In Section 7, it is shown how the Galois correspondence theorems for Galois rings, groups, Lie rings, and birings $\mathcal{G}$ acting on a field $K$ support Galois descent. They lead to theorems which establish passage from $K$-modules $V$ acted on by $\mathcal{G}$ to $K^\mathcal{G}$-modules $U = V^\mathcal{G}$—this passage being inverse to Galois ascent $V = K \otimes_{K^\mathcal{G}} U$ from $U$ to $V$ together with the corresponding action of $\mathcal{G}$ on $V$. Their generalizations from fields $K$ to commutative rings $A$ are the Galois descent Theorems 7.1, 7.2, 7.4, 7.5.

Finally, in Section 8, four successively easier problems concerned with determining simple derivation rings are formulated and considered. The hardest of these—Problem 8.1—is equivalent to the problem of determining all simple Lie rings. And the easiest—Problem 8.4—is solved by Theorem 4.2 in the finitely generated case.

1.2. Earlier work

It is instructive to review some of the more closely related earlier work.

1.2.1. Auslander–Goldman Galois extensions. The Chase–Harrison–Rosenberg correspondence

Auslander and Goldman introduce and use the notion of Galois extension of a commutative ring in [2]. Chase, Harrison, and Rosenberg then adopt and use the Auslander–Goldman Galois extensions to generalize the classical Galois correspondence theorem from fields to commutative rings [4].
Specifically, for a commutative ring $S$ and finite group $G$ of automorphisms of $S$ with fixed subring $R \equiv S^G$, $S$ is an Auslander–Goldman Galois extension of $R$ with Galois group $G$ if $S$ is $G$-strong. Here, an $R$-subalgebra $T$ of $S$ is $G$-strong if for any $g, h \in G$, the restrictions of $g, h$ to $T$ are equal if and only if $g(t)e = h(t)e$ for all $t \in T$ and all idempotents $e$ of $T$. The first part of [4, Theorem 2.3] then goes as follows.

**Theorem 1.1** (Chase–Harrison–Rosenberg correspondence theorem). *Let $S$ be an Auslander–Goldman Galois extension of $R$ with Galois group $G$. Then $G' \mapsto S^{G'}$ is a bijection from the set of subgroups of $G$ to the set of separable $G$-strong $R$-subalgebras of $S$.*

The resulting Chase–Harrison–Rosenberg Galois theory is a separable Galois theory—concerned with separable extensions—which comes into play relative to an ambient Auslander–Goldman extension $S$ of $R$ by Galois group $G$. The $G$ is finite, but not always uniquely determined by $S$.

In contrast, the Galois groups theory of Section 3 of this paper is a separable Galois theory which comes into play when $B$ is any commutative ring and $H$ is any group of automorphisms of $B$ such that $H$ acting on the spectrum of maximal ideals of $B$ has some finite orbit—as explained in Example 3.1. So, the groups $G$ of Theorem 3.1 are usually infinite.

1.2.2. The Chase–Sweedler correspondence. Kreimer–Takeuchi $J$-Galois extensions

The Chase–Sweedler Galois theory of [5] comes into play relative to an ambient $A$-object $S$ for a finite commutative Hopf algebra $A$ over a subring $R$ of $S$—rather than relative to an Auslander–Goldman extension $S$ of $R$ by Galois group $G$. The $S$ is a commutative ring together with an appropriate structure map $\alpha : S \rightarrow S \otimes A$.

The Chase–Sweedler correspondence [5, Theorem 7.6] generalizes the Chase–Harrison–Rosenberg correspondence—and is used to reobtain it.

Kreimer–Takeuchi $J$-Galois extensions $B$ of $A$ over $R$ are introduced for $J$ a Hopf algebra over a commutative ring $R$ which is finitely generated and projective as $R$-module [15]. These generalize Chase–Sweedler extensions to non-commutative algebras $B$—and lead to a natural Hopf-algebraic definition of normal basis with applications to systems of automorphisms, derivations, and higher derivations at prime characteristic.

In contrast, the Galois biring theory of Section 6 of this paper enriches the Galois rings correspondence of Section 2 between the cofinite-dimensional subfields $F$ of a commutative ring $A$ and the Galois rings $R$ of $A$ by endowing the $R$ corresponding to an $F$ with its biring structure. This is done within the biring $\text{Pres} A$ of preservations of $A$—with the $R$ corresponding to $F$ then being $\text{Pres} F A$.

1.2.3. Knus–Ojanguren descent theory

In their classical work *Théorie de la Descente et Algèbres d’Azumaya* [12], Knus and Ojanguren includes their Descente galoisienne and Descente radicielle de hauteur un for commutative algebras.

Their *Descente galoisienne* [12, pp. 44–49] for a commutative algebra extension $S/R$ and a finite group $G$ of automorphisms of $S$ such that $S$ is a projective $R$-module of finite
type such that $\text{End}_R S$ has $G$ as left $S$-module basis delivers an $S^G$-form $M^G$ of $M$ for any $S$- and $G$-module $M$ with descent action

$$g(sm) = g(s)g(m) \quad (s \in S, m \in M, g \in G).$$

In contrast, the Galois groups descent theory of this paper comes into play when $G$ is any finite-irreducible automorphism group of a commutative ring $A$—e.g., where $A$ and $G$ are constructed in the manner of Example 3.1. For such an $A$ and $G$, and for any $G$-descent module $V$ in the sense of Definition 7.2, $V^G$ is an $A^G$-form of $V$. No counterpart of the Descent galoisienne assumption described above that $G$ be an $S$-basis for $\text{End}_R(S)$ is necessary in the hypothesis of Theorem 7.2. To the contrary, often an irreducible group $G$ of automorphisms of $A$ is not $A$-independent and this condition is not met. On the other hand, it is a consequence of the irreducibility of $G$ on $A$ that $\text{End}_{A^G} A$ is the $A$-span of $G$.

Their Descente radicielle de hauteur un [12, pp. 49–53] for a commutative algebra extension $S/R$ of characteristic $p$ and a restricted Lie algebra $L$ of derivations of $S$ such that $S$ is a projective $R$-module of finite type such that $\text{End}_R S$ is generated by $L$ as ring and $S$-module delivers an $S^L$-form $M^L$ of $M$ for any $S$- and restricted $L$-module $M$ with descent action

$$d(sm) = d(s)m + sd(m) \quad (s \in S, m \in M, d \in L).$$

In contrast, the Galois Lie rings descent theory of this paper comes into play when $A$ and $D$ are constructed in the manner of Example 4.1. Then $A$ is $D$-simple and every $D$-descent module for $D$ in the sense of Definition 7.3 has an $A^D$-form $V^D$ by Theorem 7.4. No counterpart of the Descent radicielle de hauteur un assumption that $\text{End}_R(S)$ be generated as ring and $S$-module by $D$ described above is needed in the hypothesis of Theorem 7.4. Instead, it is a consequence of the irreducibility of $D$ on $A$ that $\text{End}_{A^D} A$ is the ring generated by $D$.

1.3. Conventions

General references are [1,8,16] for fields, [7] for Lie algebras, and [14,16] for coalgebras and bialgebras over fields. For a vector space $V$ over a field $F$, the zero subspace is 0. The dimension of $V$ over $F$ is $V : F$. And the identity endomorphism of $V$ is $I_V$.

Rings $R$ are assumed to be unital and associative. And $R$-modules are assumed to be unital—as are $R$-module homomorphisms.

A subfield of a ring $R$ is a unital subring of $R$ which is a field.

An algebra over a field $F$ is a ring $R$ containing $F$ as central subfield together with the induced structure as vector space over $F$.

A commutative ring (respectively algebra) is a nonzero ring (respectively algebra) $A = (A, \pi, 1_A)$ such that $ab = ba \ (a, b \in A)$.

A quasi-local ring is a commutative ring having only finitely many maximal ideals.

Throughout the paper, $A$ denotes a commutative ring.
For the purposes of this paper, a Lie ring is a Lie algebra over the prime field $\pi \equiv \mathbb{Z}_p$ of prime characteristic $p$ or the prime field $\mathbb{Q}$ of rational numbers—since the Lie rings considered in this paper are algebras over some field. A linear Lie ring is a Lie subalgebra of a linear Lie algebra on a vector space $V$ over a prime field.

A restricted linear Lie ring is a linear Lie ring $L$ of prime characteristic $p$ such that $L^p \subseteq L$.

2. Galois rings theory

The Jacobson–Bourbaki theorem establishes a bijective Galois correspondence

$$F \leftrightarrow R \equiv \text{End}_F K, \quad R \leftrightarrow F \equiv K^R$$

between the set of subfields $F$ of finite codimension of a field $K$ and the set of subrings $R$ of the endomorphism ring $\text{End} K$ of $K$ which contain $KI_A$ and are finite-dimensional over $K$. In its most concise form, the Jacobson–Bourbaki theorem states that such an $R$ is the algebra $\text{End}_F K$ of endomorphisms of $K$ over the centralizer $F = K^R$ of $R$—and that $F$ is of finite codimension in $K$.

The Jacobson–Bourbaki theorem generalizes from fields $K$ to commutative rings $A$ as follows.

**Definition 2.1.** An endomorphism ring of $A$ is a subring $R$ of the ring $\text{End} A$ of endomorphisms of $A$ which contains $AI_A$. Its centralizer is the subring $A^R \equiv \{b \in A \mid r(ab) = r(a)b \ (r \in R, \ a \in A)\}$ of $A$.

An endomorphism ring $R$ of a commutative ring $A$ is irreducible if 0 and $A$ are the only $R$-stable ideals of $A$—in which case its centralizer $A^R$ is a field by Schur’s lemma.

An endomorphism ring $R$ of $A$ is regarded as $A$-module—and is said to be finitely generated over $A$ if it is finitely generated as $A$-module.

**Definition 2.2. A Galois ring of $A$ is an irreducible endomorphism ring of $A$ which is finitely generated over $A$. A Galois ring subfield of $A$ is a subfield $F$ of $A$ of finite codimension—and the corresponding extension is a Galois ring extension.**

Evidently, the map pair $(A^-, \text{End} A)$ is a Galois correspondence—sending $F$ to $R = \text{End}_F A$ and $R$ to $F = A^R$—between the set of unital subrings $F$ of $A$ and the set of endomorphism rings $R$ of $A$. The Galois ring correspondence theorem—Theorem 2.1—establishes a bijective Galois correspondence within this one.

**Lemma 2.1.** Let $s_1, \ldots, s_n \in \text{End} A$. Suppose that $As_1 + \cdots + As_n$ contains $r_1, \ldots, r_m$ and $A$ contains $e_1, \ldots, e_m$ such that $r_i e_k = \delta_{ik} \ (1 \leq i, k \leq m)$. Then $m \leq n$.

**Proof.** Writing $r_i = \sum_j a_{ij} s_j$ and applying both sides to $e_k$ leads to...
\[ \delta_{ik} = r_i e_k = \sum_j a_{ij} s_j e_k \quad (1 \leq i, k \leq m). \]

This may be expressed as the matrix equation \((a_{ij})(s_j e_k) = I\) — \(I\) being the \(m \times m\) identity matrix over \(A\). Since \(A\) is unital and nonzero, \(A\) has a maximal ideal \(M\) — by Zorn’s lemma — and there is a homomorphism \(a \mapsto \bar{a}\) from \(A\) to the field \(\bar{A} = A/M\) whose kernel is \(M\). Under this homomorphism, the matrix equation becomes \((\bar{a}_{ij})(\bar{s}_j e_k) = \bar{I}\), \(\bar{I}\) being the \(m \times m\) identity matrix over \(\bar{A}\). Since \((\bar{a}_{ij})\) is then an \(m \times n\) matrix of rank \(m\) over a field, it follows that \(m \leq n\).

2.1. Galois rings correspondence

**Theorem 2.1** (Galois rings correspondence theorem). Let \(R\) be a Galois ring of \(A\). Then \(F \equiv A^R\) is a subfield of \(A\) of finite codimension and \(R\) is the ring \(\text{End}_F A\) of endomorphisms of \(A\) over \(F\).

**Proof.** Since \(R\) is finitely generated over \(A\), \(R = As_1 + \cdots + As_n\) with \(s_1, \ldots, s_n \in R\) for some positive integer \(n\). Since \(R\) is irreducible and contains \(AI_A\), the centralizer \(\text{End}_R A\) of \(R\) in \(\text{End} A\) is \(F = A^R\). So, by the Jacobson–Chevalley density theorem [6, 9], for \(m \geq 1\) and linearly independent \(e_1, \ldots, e_m \in A\) over \(F\), there exist \(r_1, \ldots, r_m \in R\) such that \(r_i e_k = \delta_{ik} (1 \leq i, k \leq m)\). By Lemma 2.1, it follows that \(m \leq n\). Taking such a system with \(m\) maximal, the \(e_1, \ldots, e_m\) constitute a basis for \(A\) over \(F\) — and \(A\) is finite-dimensional over \(F\). The \(E_{ij} \equiv e_i e_j (1 \leq i, j \leq m)\) then form the basis for \(\text{End}_F A\) over \(F\) such that \(E_{ij} e_k = \delta_{jk} e_i (1 \leq i, j, k \leq m)\). Since \(R\) contains \(F\) and the \(E_{ij}\) (1 \(\leq i, j \leq m\)), it follows that \(R = \text{End}_F A\).

Theorem 2.1 establishes the **Galois rings correspondence** for a commutative ring \(A\) — the bijective Galois correspondence

\[ F \leftrightarrow R \equiv \text{End}_F A, \quad R \leftrightarrow F \equiv A^R \]

between the set \(F_R\) of Galois ring subfields \(F\) of \(A\) and the set \(R\) of Galois rings \(R\) of \(A\).

**Example 2.1.** Let \(B\) be any commutative ring and let \(S\) be an endomorphism ring of \(B\) which is finitely generated over \(B\). Let \(J\) be any maximal \(S\)-stable ideal of \(B\) and take \(A \equiv B/J\). Then the ring \(R\) of endomorphisms of \(A\) induced by those of \(S\) on \(B\) is a Galois ring of \(A\). So, the hypothesis of Theorem 2.1 is satisfied and the conclusion holds.

3. Galois groups theory

The classical Galois correspondence theorem generalizes from fields \(K\) to commutative rings \(A\) as follows.
Definition 3.1. An automorphism group of $A$ is a subgroup $G$ of the group $\text{Aut}(A)$ of automorphisms of $A$. Its centralizer is the subring

$$A^G \equiv \{ b \in A \mid g(ab) = g(a)b \ (g \in G, a \in A) \} = \{ b \in A \mid g(b) = b \ (g \in R) \}$$

of $A$.

An automorphism group $G$ of $A$ is irreducible if $0$ and $A$ are the only $G$-stable ideals of $A$—in which case its centralizer $A^G$ is a field by Schur’s lemma.

A subfield $F$ of $A$ is group irreducible if the group $\text{Aut}_F A$ of automorphisms of $A$ fixing all elements of $F$ is an irreducible automorphism group of $A$.

A Galois group subfield of $A$ is a group irreducible subfield $F$ of $A$ such that $F = A^\text{Aut}_F A$—and the corresponding extension $A/F$ is a Galois group extension. So, when $A/F$ is a Galois group extension and $A$ is a field, $A/F$ is simply a Galois field extension of $F$.

A Galois group of $A$ is a group of the form $\text{Aut}_F A$ where $F$ is a Galois group subfield of $A$.

By virtue of these definitions, the map pair $(A, \text{Aut}_A)$ is a bijective Galois correspondence $G = \text{Aut}_F A$, $F = A^G$ between the set $F_G$ of Galois subfields $F$ of $A$ and the set $G$ of Galois groups $G$ of $A$.

It remains only to describe the Galois groups $G$ of $A$ and the corresponding extensions $A$ over $A^G$.

When $A$ is quasi-local, the following theorem reduces the problem of describing the Galois groups $G$ of $A$ and corresponding extensions $A$ over $A^G$—in the broad sense adopted here—to that of describing them when $A$ is a field. In fact, most such $A$ have uncountable Galois groups $G$, in which case $A$ and $G$ are described in terms of the field ideals $A_i$ of $A$ and their automorphism groups $G_i$—the latter then also being uncountable.

Theorem 3.1 (Galois groups correspondence theorem). Suppose that $A$ is quasi-local and $G$ is an irreducible automorphism group of $A$ with fixed field $F = A^G$. Then

1. $A$ is the direct sum $A = \sum_i A_i$ of finitely many ideals $A_i$ which are pairwise isomorphic Galois field extensions of $F$.
2. Relative to field isomorphisms $\alpha_i : A_i \to A_1$ ($1 \leq i \leq n$), $\text{Aut}_F A$ is the internal semi-direct product $P \prod_i G_i$ where $P$ is the symmetric group acting on $A$ by $g(a) \equiv \sum_i \alpha_i^{-1}(g(a_i))$ for $a = \sum_i a_i \in A = \sum_i A_i$ and $\prod_i G_i$ is a normal subgroup of $\text{Aut}_F A$ where $G_i$ acts as the Galois group $\text{Aut}_F A_i$ on $A_i$ and as the identity on $A_j$ ($j \neq i$).
3. The subgroup $P$ of $\text{Aut}_F A$ is unique up to conjugacy by the element of $\prod_i G_i$ corresponding to another choice of isomorphisms $\alpha_i$.
4. $P$ is a Galois group of $A$ whose corresponding Galois group subfield $F \equiv A^P$ is isomorphic to the field ideals $A_i$—and $A$ is isomorphic to $F^n$.

Proof. Since $G$ is irreducible and stabilizes the intersection $\bigcap_i M_i$ of the finitely many maximal ideals $M_i$ of $A$, the intersection $\bigcap_i M_i$ is $0$. Defining $A_i \equiv \bigcap_{j \neq i} M_j$, $A$ is then
the direct sum $A = \sum A_i$ of the finitely many ideals $A_i$—which are field extensions of $F$ by virtue of the direct sum decompositions $A = A_i \oplus M_i$. Since $G$ is irreducible and the sum $B$ of the $A_i$ which are isomorphic to $A_1$ is a $G$-stable ideal of $A$, $B = A$ and the $A_i$ are pairwise isomorphic. The subgroup $P$ of $\text{Aut}_F A$ acts as the symmetric group on the set of field ideals $\{A_1, \ldots, A_n\}$—with $g \in P$ mapping $A_i$ to $A_{g(i)}$ for all $i$. The product $\prod G_i$ of $G_i$ acting as $\text{Aut}_F A_i$ on $A_i$ and as the identity on $A_j$ ($j \neq i$) is a normal subgroup of $\text{Aut}_F A$. For any $x \in \text{Aut}_F A$, $\prod G_i$ contains $z \equiv y^{-1} x y$ where $y$ is the element of $P$ which permutes the $A_i$ the same way as does $x$—since $z$ stabilizes the $A_i$. So, $x = yz$ and $\text{Aut}_F A = P \prod G_i$. The stated unicity of $P$ follows at once. Since $F = A^P \prod G_i$, the fields $A_i$ are Galois extensions of $F$ with Galois groups $G_i$.

Since $P$ acts transitively on the field ideals $A_i$, and since any nonzero ideal of $A$ contains a field ideal, the only $P$-stable ideal of $A$ is $A$. So, $P$ is an irreducible automorphism group of $A$. The field $\overline{F} = A^P$ is a “diagonal” of the direct sum $A = \sum A_i$ which is isomorphic to the $A_i$. To see this, interpret $a = \sum a_i e_i$ as a linear combination $a = \sum a_i e_i$ of basis vectors $e_i$ with coefficients in a field isomorphic to the $A_i$ and take the field ideal isomorphisms $\alpha_i : A_i \to A_1$ to be $\alpha_i(a_i e_i) = a_i e_1$ ($1 \leq i \leq n$). Then the action

$$g \left( \sum_i a_i e_i \right) \equiv \sum_i \alpha_{g(i)}^{-1} \alpha_i(a_i)$$

interprets as

$$g \left( \sum_i a_i e_i \right) \equiv \sum_i \alpha_{g(i)}^{-1} \alpha_i(a_i e_i) = \sum_i \alpha_{g(i)}^{-1} (a_i e_1) = \sum_i a_i e_{g(i)}.$$

So,

$$g \left( \sum_i a_i e_i \right) = \sum_i a_i e_{g(i)} \quad (g \in P)$$

and $\sum_i a_i e_i \in \overline{F} = A^P$ if and only if the coefficients $a_i$ are all equal. This shows that $\overline{F}$ is a “diagonal” isomorphic to the field ideals $A_i$ and $A$ is isomorphic to $\overline{F}^n$.

Any automorphism of $A$ which leaves fixed the elements of $\overline{F} = A^P$ is of the form $x = yz$ with $y \in P$ and $z \in \prod G_i$. Since $z = y^{-1} x$ fixes them as well, $z$ also must fix all elements of all $A_i$, that is, $z$ must be the identity and $x = y \in P$. So, $P = \text{Aut}_\overline{F} A$ and $P$ is a Galois group of $A$.  \( \square \)

**Example 3.1.** Let $B$ be any commutative ring and let $H$ be any group of automorphisms of $B$ such that $H$ acting on $\text{Spec}_{\text{max}}(B)$—the spectrum of maximal ideals of $B$—has some finite orbit $M_i$. Let $J$ be any maximal $H$-stable ideal of $B$ containing the intersection of the $M_i$, take $A \equiv B/J$, and take $G$ to be the group of automorphisms of $A$ induced by $H$. Then $A$ is quasi-local and $G$-simple. So, the hypothesis of Theorem 3.1 is satisfied and the conclusion holds.
In particular, when $H$ is any finite group of automorphisms of any commutative ring $B$, every orbit of $H$ in $\text{Spec}_{\text{max}}(B)$ leads to corresponding $A$ and $G$ satisfying the hypothesis of Theorem 3.1.

**Corollary 3.1.** Suppose that $G$ is a finite-irreducible automorphism group of $A$ and let $F \equiv A^G$. Then

1. $A$ is the direct sum $A = \sum_i A_i$ of finitely many ideals $A_i$ which are pairwise isomorphic finite-dimensional Galois field extensions of $F$.
2. Relative to field isomorphisms $\alpha_i : A_i \to A_1$ (1 \leq i \leq n), $\text{Aut}_F A$ is the internal semi-direct product $P \prod_i G_i$ where $P$ is a symmetric group acting on $A$ by $g(a) \equiv \sum_i \alpha_{g(i)}^{-1} \alpha_i(a_i)$ for $a = \sum_i a_i \in A = \sum_i A_i$ and $\prod_i G_i$ is a normal subgroup of $\text{Aut}_F A$ where $G_i$ acts as the Galois group $\text{Aut}_F A_i$ on $A_i$ and as the identity on $A_j$ ($j \neq i$).
3. The subgroup $P$ of $\text{Aut}_F A$ is unique up to conjugacy by the element of $\prod_i G_i$ corresponding to another choice of isomorphisms $\alpha_i$.
4. $P$ is a Galois group of $A$ whose corresponding Galois group subfield $\overline{F} \equiv A^P$ is isomorphic to the field ideals $A_i$—and $A$ is isomorphic to $\overline{F}^n$.

**Proof.** The $A$-span $R = AG$ of $G$ is an endomorphism ring of $A$ since $(ag)(bh) = ag(b)gh$ ($a, b \in A$; $g, h \in G$). Since $G$ is finite and irreducible, $R$ is then a Galois ring of $A$. Moreover, $A^R = A^G = F$ by the computations

\[
\begin{align*}
b \in A^R & \Rightarrow g(b) = g(1b) = g(1)b = b \quad (g \in G) \quad \Rightarrow \quad b \in A^G, \\
b \in A^G & \Rightarrow g(ab) = g(a)g(b) = g(a)b \quad (a \in A, \ g \in G) \quad \Rightarrow \quad b \in A^R.
\end{align*}
\]

By Theorem 2.1, $A : F$ is finite. So, $A$ has only finitely many maximal ideals and Theorem 3.1 applies. $\square$

**Remark 3.1.** When $A$ has only finitely many maximal ideals and $G$ is an irreducible automorphism group of $A$ with finite orbits, the $A_i$ in Theorem 3.1 are algebraic field extensions of the field $F \equiv A^G$. To see this, simply note that the polynomial $f(X) \equiv (X - a_1) \cdots (X - a_m)$ whose roots are the elements $a_1, \ldots, a_m$ of the orbit of $a \in A_i$ under $G$ is fixed by $G$, so its coefficients are in $F$. But then $a$ satisfies a nonzero polynomial with coefficients in the field $F$. So, every element $a$ of the field extension $A_i$ of $F$ is algebraic over $F$.

**Remark 3.2.** When $A$ has only finitely many maximal ideals, $G$ is an irreducible automorphism group of $A$, and $A$ is algebraic over the field $F \equiv A^G$, then the $A_i$ in Theorem 3.1 are algebraic field extensions of $A^G$. Then $G$ is the product of the finite group $P$ and a normal subgroup $\prod_i G_i$ whose orbits are finite, so the orbits of $G$ are finite as well.

**Remark 3.3.** Suppose $A$ is the direct sum $A = \sum_i A_i$ of finitely many ideals $A_i$ which are algebraically closed field extensions of a field $F$. Relative to isomorphisms $\alpha_i : A_i \to A_1$
regard the symmetric group $P \equiv S_n$ as an automorphism group of $A$ by way of the action $g(a) \equiv \sum_i \alpha(g(i))^{-1} \alpha(g(i))$ for $a = \sum_i a_i \in A = \sum A_i$ and $g \in P$. Then $P$ is irreducible—since any nonzero $P$-stable ideal of $A$ contains some $A_i$, hence contains all $A_i$, by the transitivity of $P$ on the $A_i$. So, $P$ is a Galois group of $A$—as is the larger $\text{Aut}_F A$. The corresponding Galois group subfield $\overline{F} \equiv A^P$ is an algebraic closure of $F$—being isomorphic to the $A_i$—with $P = \text{Aut}_F A$. It depends on $P$. The purely inseparable closure $F_{\text{rad}}$ of $F$ in $\overline{F}$ is the Galois group subfield $A^{\text{Aut}_F A}$—and so does not depend on $P$. Letting $A_{\text{sep}}$ be the sum of the separable closures of $F$ in the $A_i$, $A = A_{\text{sep}} \otimes_F F_{\text{rad}}$ (internal tensor product over $F$).

### 4. Galois Lie rings theory

For fields $K$ of prime characteristic $p$, the Jacobson differential correspondence theorem establishes a bijective Galois correspondence

$$F \leftrightarrow D \equiv \text{Der}_F K, \quad D \leftrightarrow F \equiv K^D$$

between the set of subfields $F$ of finite codimension of a field $K$ such that $K^p \subseteq F$ and the set of Lie subrings $D$ of the derivation ring $\text{Der}(K)$ of $K$ which contain $KI$, are finite-dimensional over $K$, and are restricted (as linear Lie algebras over the prime field).

In its most concise form, the Jacobson differential correspondence theorem states that such a $D$ is the Lie algebra $\text{Der}_F K$ of derivations of $K$ over the centralizer $F = K^D$ of $D$—and that $F$ is of finite codimension in $K$.

The Jacobson differential correspondence theorem generalizes from fields $K$ to commutative rings $A$ of prime characteristic $p$ as follows.

**Definition 4.1.** A derivation ring of a commutative ring $A$ is an $A$-submodule and Lie subring $D$ of the ring $\text{Der}(A)$ of derivations of $A$. Its centralizer or ring of constants is the subring

$$A^D = \{ b \in A \mid d(ab) = d(a)b \ (d \in D, \ a, b \in A) \} = \{ b \in A \mid d(b) = 0 \ (d \in D) \}.$$ 

A derivation ring is the derivation ring of some commutative ring $A$.

Evidently, the map pair $(A^-, \text{Der}_-) A$ is a Galois correspondence $D = \text{Der}_F A$, $F = A^D$ between the set of unital subrings $F$ of $A$ and the set of derivation rings $D$ of $A$. The Galois Lie ring correspondence theorem—Theorem 4.2—establishes a bijective Galois correspondence within this one.

**Definition 4.2.** A derivation ring $D$ of $A$ is irreducible if $D \neq 0$ and $0$, $A$ are the only $D$-stable ideals of $A$. An irreducible derivation ring is an irreducible derivation ring $D$ of some $A$. A finitely generated irreducible derivation ring is an irreducible derivation ring $D$ of some $A$ which is finitely generated as $A$-module.
The ring of constants $A^D$ of an irreducible derivation ring $D$ of $A$ is a field by Schur’s lemma.

4.1. Galois Lie rings and their dual generating systems

Definition 4.3. A Galois Lie ring of $A$ is a restricted irreducible derivation ring $D$ of $A$ which is finitely generated as $A$-module. A Galois Lie ring subfield of $A$ is any subring $F$ of the form $F = A^D$ where $D$ is a Galois Lie ring of $A$—and the corresponding extension $A/F$ is called a Galois Lie ring extension. The set of Galois Lie rings (respectively Galois Lie ring subfields) of $A$ is denoted $D$ (respectively $F_D$).

Definition 4.4. A dual system of rank $m$ in a derivation ring $D$ of $A$ is a paired set of elements $d_1, \ldots, d_m, e_1, \ldots, e_m \in A$ such that $d_i e_k = \delta_{ik} (1 \leq i, k \leq m)$. A dual system of $A$ is a dual system in the derivation ring $\text{Der}(A)$ of $A$.

Definition 4.5. A dual generating system for a derivation ring $D$ of $A$ is a dual system $d_1, \ldots, d_m, e_1, \ldots, e_m \in A$ in $D$ such that $D = Ad_1 + \cdots + Ad_m$.

For $D \in D$, $D$ contains a dual system of rank 0—the vacuous one. Moreover, since $D$ is generated as $A$-module by a finite number $n$ of elements, every dual system in $D$ has rank $m \leq n$—by Lemma 2.1. From these two facts, $D$ has a maximal dual system—one of maximal rank. Consequently, the following theorem establishes, in particular, that $D$ has a dual generating system.

Theorem 4.1. For $D \in D$, every maximal dual system in $D$ is a dual generating system for $D$.

Proof. Suppose that $d_1, \ldots, d_m, e_1, \ldots, e_m \in A$ with $m > 0$ is a maximal dual system in $D$. Let $D' = \{d' \in D \mid de' = 0 (1 \leq j \leq m)\}$. Then $D = Ad_1 + \cdots + Ad_m + D'$. After all, each $d \in D$ can be written as $d = d(e_1)d_1 + \cdots + d(e_m)d_m + d'$ for some $d'$—and that $d'$ vanishes at $e_1, \ldots, e_m$ since $de_j = (d(e_1)d_1 + \cdots + d(e_m)d_m)e_j (1 \leq j \leq m)$.

The maximality of $m$ leads to the conclusion $D' = 0$—in two steps. The first step is to show that $D'$ maps $A$ into the nil radical $N$ of $A$; and the second step is then to show that $A(D'A)$ is a $D$-stable ideal of $A$ contained in $N$. Since $D$ is irreducible, the ideal $A(D'A)$ must then be 0, that is, $D' = 0$.

For the first step, suppose that $D'A$ is not contained in $N$ and take $d \in D'$, $e_{m+1} \in A$ such that $\hat{f} = d(e_{m+1})$ is not nilpotent. Since the derivations in $D$ vanish at $p$th powers, $a \equiv f^p$ is in $A^D = F$. Since $\hat{f}$ is not nilpotent, $a \neq 0$. But then $1 = a^{-1} f^{p-1} \hat{f}$ and $\hat{f}$ is invertible in $A$. Replacing $d$ by $d_{m+1} = f^{-1}d, d_{m+1}e_{m+1} = 1$. Since $d \in D'$, $d_{m+1}e_j = 0 (1 \leq j \leq m)$. But the existence of such $d_{m+1}, e_{m+1}$ contradicts the maximality of $m$. So, $D'A$ is contained in $N$.

For the second step, note that $D'$ is a Lie subalgebra of $D$ whose Lie algebra normalizer $E$ in $D$ contains the $d_1, \ldots, d_m$. After all, for $d' \in D'$ and $1 \leq i, j \leq m$, $[d_i, d']e_j = d_i d' e_j - d' d_i e_j = d_i 0 - d' \delta_{ij} = 0$. It follows that $D = Ad_1 + \cdots + Ad_m + D' \subseteq AE \subseteq D$ and $D = AE$. Since $E$ normalizes $D'$, it stabilizes $D'A$ by the identity $d(d'a) =$
\[ [d, d']a - d'(da) \in D' A \ (d \in E, \ d' \in D', \ a \in A) \]. But then it also stabilizes the ideal \( A(D' A) \) by the identity \( d(ab) = d(a)b + ad(b) \in A(D' A) + A(E(D' A)) \subseteq A(D' A) \) \( (d \in E, \ a \in A, b \in D' A) \). Finally, since \( D' A \subseteq N \) by the first step, the \( E \)-stable ideal \( A(D' A) \) is contained in \( N \)—and so is a proper \( E \)-stable ideal. Since \( D = AE \), it is then a proper \( D \)-stable ideal as well. Since \( D \) is irreducible, it follows that \( A(D' A) = 0 \)—and so \( D' = 0 \) as well.

Since \( D = Ad_1 + \cdots + Ad_m + D' \), the conclusion that \( D' = 0 \) establishes the decomposition \( D = Ad_1 + \cdots + Ad_m \). So, \( d_1, \ldots , d_m \in D, \ e_1, \ldots , e_m \in A \) is a dual generating system for \( D \). \( \square \)

**Lemma 4.1.** For \( D \in D \), \( A \) is finite-dimensional over \( A^D \).

**Proof.** The methods of [8, Theorem 19, p. 186] generalize to show that the \( A \)-span of the monomials \( d_1^{i_1} \cdots d_m^{i_m} \ (0 \leq i_1, \ldots , i_m \leq p - 1) \) for \( d_1, \ldots , d_m \) an \( A \)-module generating set for \( D \) is a Galois ring \( R \). By Theorem 2.1, \( A \) is then a finite-dimensional extension of the field \( A^D \). \( \square \)

**Definition 4.6.** Let \( B \) be a commutative ring. Then a truncated polynomial algebra over \( B \) in the \( e_i \) with respect to \( c_i \in B \ (1 \leq i \leq m) \) is \( B[e_i \mid 1 \leq i \leq m] \equiv B[X_i \mid 1 \leq i \leq m]/(X_i - c_i \mid 1 \leq i \leq m) \). When the \( c_i \) are all 0, \( B[e_i \mid 1 \leq i \leq m] \) is a truncated polynomial algebra over \( B \). When the \( c_i \) are not all 0, \( B[e_i \mid 1 \leq i \leq m] \) is a truncated polynomial algebra over \( B \) with respect to constants.

**Theorem 4.2** (Galois Lie rings correspondence theorem). For \( D \in D \), \( A \) is a finite-dimensional truncated polynomial algebra over \( F \equiv A^D \) with respect to constants—and \( D = \text{Der}_F A \).

**Proof.** By Lemma 4.1, \( A \) is finite-dimensional over \( F \). Consequently, \( A \) has a minimal ideal. Since \( A \) is also differentiably simple, \( A \) is a truncated polynomial algebra over some simple ring \( B \)—in the sense of Definition 4.6—by the Block’s theorem on differentiably simple algebras with minimal ideal [3]. This simple ring \( B \) must be a purely inseparable field extension of \( F \)—since \( A^D \subseteq F \). It follows that \( A \) is a truncated polynomial algebra over \( F \) with respect to constants. To see that \( D = \text{Der}_F A \), suppose that \( d_1, \ldots , d_m \in D, \ e_1, \ldots , e_m \in A \) with \( m \geq 0 \) is a dual generating system for \( D \). Since \( A \) is finite-dimensional over \( F \), \( \text{Der}_F A \) is in \( D \). So, it is possible to extend the dual generating system for \( D \) to a maximal dual system \( d_1, \ldots , d_m^* \in \text{Der}_F A, \ e_1^*, \ldots , e_m^* \in A \) in \( \text{Der}_F A \)—with \( m' \geq m \).

The extended system is then a dual generating system for \( \text{Der}_F A \) by Theorem 4.1. If \( m' > m \), then \( d_i e_{m+1} = 0 \ (1 \leq i \leq m) \) and \( e_{m+1} \in A^D = F \equiv A^{\text{Der}_F A} \). But this is impossible since \( d_{m+1} e_{m+1} = 1 \) is not 0. But then \( m' = m \)—so that \( d_1, \ldots , d_m \in D, \ e_1, \ldots , e_m \in A \) is a dual generating system for both \( D \) and \( \text{Der}_F A \). This establishes that \( D = \text{Der}_F A \). \( \square \)

Theorem 4.2 establishes the **Galois Lie ring correspondence** for a commutative ring \( A \)—the bijective Galois correspondence

\[ F \leftrightarrow D \equiv \text{Der}_F A, \quad D \leftrightarrow F \equiv A^D \]
between the set $F_D$ of Galois Lie ring subfields $F$ of $A$ and the set $D$ of Galois Lie rings $D$ of $A$—with $F$ being a Galois Lie ring subfield of $A$ if and only if $A$ is a finite-dimensional truncated polynomial algebra over $F$.

Example 4.1. Let $B$ be any commutative ring and let $E$ be a restricted derivation ring of $B$ which is finitely generated over $B$. Let $J$ be any maximal $E$-stable ideal of $B$ and take $A ≡ B/J$. Then the derivation ring $D$ of $A$ induced by $E$ is a Galois Lie ring of $A$. So, the hypothesis of Theorem 4.2 is satisfied and the conclusion holds.

5. Galois Lie rings theory and derivation ring forms

The Galois Lie ring correspondence Theorem 4.2 was proved using the Galois ring correspondence Theorem 2.1 and Block’s theorem on differentiably simple algebras with minimal ideal. It also surfaces independently as Corollary 5.1 to the main Theorem 5.3 of the following Lie ring Galois theory based on derivation ring forms—which depends neither on Theorem 2.1 nor on Block’s theorem.

Definition 5.1. A derivation ring form of $A$ is a commutative Lie subring $L$ of $\text{Der}(A)$ such that $F ≡ AL$ is a field, $L$ is finite-dimensional over $F$, and $L^p = 0$.

An $F$-form of a module $D$ for a commutative algebra $A$ over a field $F$ is an $F$-subspace $L$ of $D$ such that the bilinear pairing over $F$ sending $a, d$ ($a ∈ A, d ∈ L$) to $ad$ presents $D$ as an internal tensor product $A ⊗_F L$. So, when $L$ is finite-dimensional over $F$, $L$ is an $F$-form of $D$ if and only if any basis $d_1, ..., d_m$ for $L$ over $F$ is a free basis for $AL$ over $A$.

Lemma 5.1. Let $L$ be a derivation ring form of $A$ with $F = A^L$. Then $L$ is an $F$-form of $AL$.

Proof. Suppose that $a_1d_1 + ... + a_md_m = 0$ where the $a_i$ are in $A$ with not all of them 0. Since $L$ is abelian, it follows that $x(a_1d_1 + ... + a_md_m) = 0$ for all $x ∈ L$. Since the $p$-powers of the $x ∈ L$ are 0, there exists a product $x_n...x_1$ of maximal length $n ≥ 0$ of the $x_j$’s in $L$ such that the $b_i ≡ x_n...x_1a_i$ are not all 0. Since $L$ is abelian, successive application of the $x_1, ..., x_n$ to the equation $a_1d_1 + ... + a_md_m = 0$ leads to the equation $b_1d_1 + ... + b_md_m = 0$ where the $b_i$ are in $A^L = F$—contrary to the linear independence of the $d_i$ over $F$. So, the $d_i$ form a free basis for $D$ over $A$.

Theorem 5.1. For $D ∈ D$ with $F = A^D$, $D$ contains a derivation ring form $L$ of $A$ which is an $F$-form of $D$. In fact, $L ≡ Fd_1 + ... + Fd_m$ is such a derivation ring form of $A$ for any dual generating system $d_1, ..., d_m ∈ D, e_1, ..., e_m ∈ A$ for $D$. Conversely, when $L$ is a derivation ring form of $A$, $D ≡ AL$ is in $D$.

Proof. By Theorem 4.1, $D$ has a dual generating system $d_1, ..., d_m ∈ D, e_1, ..., e_m ∈ A$. For any such dual generating system, let $L ≡ Fd_1 + ... + Fd_m$. Then $L$ is a derivation ring form of $A$. To see this, note that the evident equalities
Theorem 5.2. Let ideal dimensional Lie subalgebra of Der nil linear transformations on Since \(d\) with respect to \(c\in A\) and \(Aj\) to \(a\) contained in those for \(A\) to be a derivation ring of \(A\) and set \(D\equiv AL\). Then \(D\) is a derivation ring of \(A\) which is finitely generated as \(A\)-module, so it remains only to show that \(D\) is irreducible on \(A\). Since \(D\) contains \(L\), it suffices to show instead that \(L\) is irreducible on \(A\). To this end, let \(B\) be a nonzero \(L\)-stable ideal of \(A\). Since \(L\) is nonzero finite-dimensional abelian with \(L^p=0\), \(L\) acts as a finite-dimensional space of commuting nil linear transformations on \(B\) and there exists a nonzero \(b\in B\) with \(Lb=0\). Then \(b\) is a nonzero element of the field \(A^L=F\). Consequently, \(B\) contains \(Fb=F^p\) and \(1\in B\). But an ideal \(B\) containing the identity of \(A\) must be \(A\). So, \(B=A\) and \(D\) is irreducible on \(A\).

Let \(d\in Der(A)\) and \(e\in A\) where \(d^p=0\) and \(d(e)=1\)—and let \(B\equiv A^d\). Then \(A=B[e]\) and \(A\) is the truncated polynomial algebra in \(e\) over \(B\) with respect to some \(c\in B\), that is, there is an isomorphism over \(B\) from \(A\) to \(B[X]/(X^p=c)\) mapping \(e\) to \(X\equiv X+(X^p=c)\).

Proof. Since \((d(e))^p=0\), \(c\equiv e^p\) is in \(A^d=B\). There can be no \(B\)-linear relation \(b_0+b_1e+\cdots+b_ne^n=0\) of the powers \(1, e, \ldots, e^{p-1}\) of \(e\) with some nonzero \(b_0\) and minimal length \(n\leq p-1\)—since there would then be one shorter length, namely, \(b_1+2b_2e+\cdots+nb_ne^{n-1}=0\) obtained by applying \(d\). So, the powers \(1, e, \ldots, e^{p-1}\) of \(e\) are linearly independent over \(B\) and \(B[e]\) is the truncated polynomial algebra in \(e\) over \(B\) with respect to \(c\).

To show that \(A=B[e]\), it suffices to show by induction that the Engel subspaces \(A_0=F, A_{n+1}=\{a\in A \mid d(a)\in A_n\}\) of the nilpotent derivation \(d\) on \(A\) with \(d^p=0\) are contained in those for \(B[e]\)—namely \(B[e]_0=F, B[e]_{n+1}=\{f\in B[e]\mid d(f)\in B[e]_{n}\}\) for \(1\leq n\leq p-2\). For \(j=0\), \(A_0=F=\{B[e]_0\}\) by definition—so assume \(0<j\leq p-2\) and \(A_j=B[e]_j\). Take any \(a\in A_{j+1}\). Then \(da\in A_j=B[e]_j\). Integrating \(d(a)\) in \(B[e]_j\) with respect to \(d\) produces \(f\in B[e]_{j+1}\) such that \(d(a)=d(f)\). But then \(d(a-f)=0\) and \(a-f\in A^d=B\). So, the \(a\in f+B\) are contained in \(B[e]_{j+1}\). This being true for all such \(a\), it follows that \(A_{j+1}\subseteq B[e]_{j+1}\). This completes the induction step, so \(A=A_{p-1}=B[e]_{p-1}=B[e]\).
Theorem 5.3. Let $L$ be a derivation ring form of $A$ with $F = A^L$. Then $\text{Der}_F A \in D$. $L$ is an $F$-form of $\text{Der}_F A$, and for every basis $d_1, \ldots, d_m$ for $L$ over $F$, there exist $e_1, \ldots, e_m \in A$ such that $d_1, \ldots, d_m \in L$, $e_1, \ldots, e_m$ is a dual system of $A$ with
\[
A = F[e_1] \otimes_F \cdots \otimes_F F[e_m],
\]
and $F[e_i]$ is the truncated polynomial algebra in $e_i$ with respect to some $c_i \in F$ for $1 \leq i \leq m$.

**Proof.** The proof is by induction on $m$—and is evident when $m = 0$ with $A = F$. If $m = 1$, then $L = Fd_1$, $F = A^{d_1}$, there exists $e_1$ such that $d_1(e_1) = 1$, and $A = F[e_1]$ is the truncated polynomial algebra with respect to some $c_1 \in F$ by Theorem 5.2. Thus, $\text{Der}_F A = F[e_1]d_1 = AL$ and $\text{Der}_F A \in D$. Suppose next that $m > 1$—and that the theorem holds for derivation ring forms of algebras of dimension $m - 1$ or less. For $1 \leq i \leq m$, let $L_i = Fd_1 + \cdots + Fd_i + \cdots + Fd_m$ (sum of $m$ terms with the $i$th removed). If $A^{L_i} = F$, then $\text{Der}_F A = AL_i$ by the induction hypothesis. But then $d_i \in AL_i$. This contradicts Lemma 5.1, according to which the $F$-basis $d_1, \ldots, d_m$ for $L$ is a $A$-basis for $AL$. It follows from this and Theorem 5.2 that $A^{L_i} \neq F$ with $A^{L_i}d_i = F$ and $A^{L_i} = F[e_j]$ for some $e_j \in A^{L_i}$ with $d_i(e_j) = 1$—for $1 \leq i \leq m$. But then the duality $d_j(e_i) = \delta_{ij}$ holds and

1. $A = A^{d_m}[e_m]$—truncated polynomial algebra in $e_m$ over $A^{d_m}$ with respect to $c_m = e_m^p$;
2. $A^{d_m} = F[e_1] \otimes_F \cdots \otimes_F F[e_m-1]$—where the $F[e_j]$ are truncated polynomial algebras in $e_j$ over $F$ with respect to $c_j = e_j^p$.

This is by Theorem 5.2 and the induction assumption. Consequently, $\text{Der}_F A \in D$. $L$ is an $F$-form of $\text{Der}_F A$, and there exist $e_1, \ldots, e_m \in A$ such that $d_1, \ldots, d_m \in L$, $e_1, \ldots, e_m$ is a dual system of $A$ with
\[
A = A^{d_m}[e_m] = F[e_1] \otimes_F \cdots \otimes_F F[e_m-1][e_m] = F[e_1] \otimes_F \cdots \otimes_F F[e_m],
\]
where the $F[e_i]$ are truncated polynomial algebras in $e_i$ with respect to $c_i \in F$ for any $1 \leq i \leq m$. □

Theorem 4.2 now reappears as the following corollary.

**Corollary 5.1** (Galois Lie rings correspondence theorem). For $D \in D$, $A$ is a finite-dimensional truncated polynomial algebra over $F = A^D$ with respect to constants—and $D = \text{Der}_F A$.

**Proof.** Every Galois Lie ring $D$ of $A$ has a derivation ring form $L$ by Theorem 5.1. But then $D = \text{Der}_F A$ and $A$ is a truncated polynomial algebra over $F$ by Theorem 5.3. □
6. Galois birings theory

The Galois rings correspondence

\[ F \mapsto R \equiv \text{End}_F A, \quad R \mapsto F \equiv A^R, \]

between the finite-codimensional subfields \( F \) of a commutative ring \( A \) and the Galois rings \( R \) of \( A \) can be enriched by imposing biring structures on the Galois rings \( R \) of \( A \) which reflect the structures of the corresponding ring extensions \( A/A^R \).

6.1. The biring of preservations of \( A \) over \( F \)

The preservation sets of \( A \) over a subfield \( F \) are the counterparts for commutative rings of the coclosed sets of \( K/k \)-bialgebras of [15,16].

**Definition 6.1.** A preservation set of \( A \) over \( F \) is a subset \( H \) of \( \text{End}_F A \) such that for each \( x \in H \) there exist finitely many \( i, x_i, x_j \) in \( H \) such that \( x(ab) = \sum_i i x(a) x_i(b) \) for all \( a, b \in A \).

When \( H \) and \( H' \) are preservation sets of \( A \) over \( F \), so is the set \( HH' \) of products \( hh' \) (\( h \in H, h' \in H' \)). For if finitely many \( x \) and \( x_i, x_j \) in \( H \) satisfy \( x(ab) = \sum_i i x(a) x_i(b) \) for all \( a, b \in A \), and finitely many \( y \) and \( y_j, y_j \) in \( H' \) satisfy \( y(ab) = \sum_j j y(a) y_j(b) \) for all \( a, b \in A \), then the finitely many \( xy \) and \( x_i y_j, x_i y_j \) in \( HH' \) satisfy

\[ (xy)(ab) = \sum_{i,j} i x_j y(a) x_i y_j(b) \]

for all \( a, b \in A \).

Arguing in like fashion, when \( H \) and \( H' \) are preservation sets of \( A \) over \( F \), so are the set \( -H' \) of negatives \( -h' \) (\( h' \in H' \)) and the set \( H + H' \) of sums \( h + h' \) (\( h \in H, h' \in H' \)).

It follows that \( \text{Pres}_F A \) is a subring of \( \text{End}_F A \). Moreover, since the sets \( \{a I_A, I_A\} \) (\( a \in A \)) are preservation sets of \( A \) over \( F \), it contains \( A I_A \). So, \( \text{Pres}_A \) is an endomorphism ring of \( A \) in the sense of Definition 2.1.

As the union of preservation sets of \( A \) over \( F \), \( \text{Pres}_F A \), too, is a preservation set of \( A \) over \( F \). The following lemma shows, for \( F \) finite-codimensional, that \( \text{Pres}_F A \) may be endowed with the structure of coalgebra over \( A \).

**Lemma 6.1.** Suppose that \( F \) is a finite-codimensional subfield of \( A \). Then finitely many \( i, x_i \) and finitely many \( j, y_j \) in \( \text{End}_F A \) satisfy the equations

\[ \sum_i i x(a) x_i(b) = \sum_j j y(a) y_j(b) \quad (a, b \in A) \]

if and only if
\[ \sum_i i x \otimes_A x_i = \sum_j j y \otimes_A y_j. \]

**Proof.** Suppose first that \( \sum_i i x(a) x_i(b) = \sum_j j y(a) y_j(b) \) \((a, b \in A)\). Select a basis \( e_r \) for \( A \) over \( F \)—and let \( z_r \in \text{End} \ A \) be defined by the conditions \( z_r(e_s) = \delta_{rs} \). Then each \( z \in \text{End} \ A \) decomposes uniquely as \( z = \sum_r z(e_r) z_r \)—and the \( z_r \) form a basis for \( \text{End} \ A \) over \( A \). Writing \( x_i = \sum_r x_i r z_r \) and \( y_j = \sum_r y_j r z_r \) for all \( i \) and \( j \) leads to

\[ \sum_r \sum_i i x(a) x_i r z_r = \sum_r \sum_j j y(a) y_j r z_r. \]

By the \( A \)-independence of the \( z_r \), this, in turn, leads to

\[ \sum_i i x(a) x_i r = \sum_j j y(a) y_j r \quad (a \in A), \]

\[ \sum_i x_i r x = \sum_j y_j r y \]

for all \( r \). But then

\[ \sum_r \left( \sum_i x_i r x \right) \otimes_A z_r = \sum_r \left( \sum_j y_j r y \right) \otimes_A z_r \]

and

\[ \sum_i i x \otimes_A \left( \sum_r x_i r z_r \right) = \sum_j j y \otimes_A \left( \sum_r y_j r z_r \right), \]

which establishes that \( \sum_i i x \otimes_A x_i = \sum_j j y \otimes_A y_j. \)

Suppose, conversely, that \( \sum_i i x \otimes_A x_i = \sum_j j y \otimes_A y_j. \) For any \( a, b \in A \), the map \((x, y) \mapsto x(a)y(b)\)

is an \( A \)-bilinear pairing from \( \text{End} \ A \times \text{End} \ A \) to \( A \). Consequently, there is an \( A \)-linear map

\[ \rho : \text{End} \ A \otimes_A \text{End} \ A \to A \]

such that \( \rho(x \otimes_A y) = x(a)y(b) \). Since \( \sum_i i x \otimes_A x_i = \sum_j j y \otimes_A y_j \), it follows that

\[ \sum_i i x(a) x_i(b) = \sum_j j y(a) y_j(b) \quad (a, b \in A). \]

For \( F \) a finite-codimensional subfield of \( A \), Lemma 6.1 ensure that \( \Delta(x) \in \text{Pres}_F A \otimes_A \text{Pres}_F A \) is well defined for \( x \in \text{Pres}_F A \) by...
\[ \Delta(x) \equiv \sum_i i_x \otimes_A x_i, \]

where \( i_x, x_i \) are finitely many elements of \( \text{Pres}_F A \) such that

\[ x(ab) = \sum_i x(a)x_i(b) \quad (a, b \in A). \]

Defining \( \varepsilon(x) \equiv x(1_A) \) \( (x \in \text{Pres}_F A) \), \( \text{Pres}_F A = (\text{Pres}_F A, \Delta, \varepsilon) \) is then a coalgebra over \( A \)—meaning that the coproduct and coidentity maps

\[ \Delta(x) = \sum_i i_x \otimes_A x_i \quad (x \in \text{Pres}_A), \]
\[ \varepsilon(x) = x(1_A) \quad (x \in \text{Pres}_A) \]

satisfy the coassociativity and coidentity laws which generalize naturally those for coalgebras over \( A \) when \( A \) is a field \([14,16]\). These laws for \( \text{Pres}_F A \) follow at once from the associativity and identity laws for \( A \) and the above definition of \( \Delta \) and \( \varepsilon \).

**Definition 6.2.** For \( F \) a finite-codimensional subfield of \( A \), the biring of preservations of \( A \) over \( F \) is \( \text{Pres}_F A \) as ring and coalgebra \((\text{Pres}_F A, \pi, I_A, \Delta, \varepsilon)\) over \( A \).

More generally, whenever \( F \) is a subfield of \( A \) and \( \text{Pres}_F A \) may be regarded as coalgebra over \( A \) with coidentity \( \varepsilon(x) = x(1_A) \) and coproduct \( \Delta(x) \) \( (x \in \text{Pres}_F A) \) such that

\[ \Delta(x) \equiv \sum_i i_x \otimes_A x_i \]

if and only if \( i_x, x_i \) are finitely many elements of \( \text{Pres}_F A \) such that

\[ x(ab) = \sum_i x(a)x_i(b) \quad (a, b \in A), \]

\((\text{Pres}_F A, \pi, I_A, \Delta, \varepsilon)\) is called the biring of preservations of \( A \) over \( F \). Examination of the proof of Lemma 6.1 shows that such a \( \Delta \) exists when \( \text{End}_F A \) has an \( A \)-basis. So, this condition is always met when \( \text{End}_F A \) has an \( A \)-basis, e.g., when \( A \) is any field extension of a field \( F \).

### 6.2. Galois birings correspondence

Theorem 2.1 now takes on the form of the following Theorem 6.1, which shows that the Galois ring \( R \) corresponding to a subfield \( F \) of \( A \) of finite codimension may be endowed with the biring structure \((R, \Delta, \varepsilon) = (\text{Pres}_F A, \Delta, \varepsilon)\).
**Theorem 6.1** (Galois birings correspondence theorem). Let $R$ be a Galois ring of a commutative ring $A$. Then $F \equiv A^R$ is a subfield of $A$ of finite codimension and $R = \text{Pres}_F A = \text{End}_F A$.

**Proof.** By Theorem 2.1, $F \equiv A^R$ is a subfield of $A$ of finite codimension and $R = \text{End}_F A$. So, it remains to show that $\text{Pres}_F A = \text{End}_F A$. This is seen by revisiting the proof of [16, Theorem 5.3.10] in the present context—with $A$ in place of $K$. Although $F$ is a field and the extension $A/F$ is finite-dimensional, due care must be exercised since $A$ is no longer assumed to be a field.

With $R = \text{End}_F A$, let $R^* \equiv R^*(A) \equiv \text{Hom}_A(R, A)$ be the dual of $R$ with coefficients in $A$. Let the $e_i$ be a basis for $A$ over $F$ and let the $r_i$ be the elements of $R$ defined by the condition that $r_i(e_j) = \delta_{ij}$. Since each $x \in R$ can be written uniquely as $x = \sum_i x(e_i)r_i$, the $r_i$ are an $A$-basis for $R$. Defining $\hat{a} \in R^*$ by $\hat{a}(x) \equiv x(a)$ ($x \in R$) for $a \in A$, the $\hat{e}_i$ satisfy $\hat{e}_j(r_i) = r_i(e_j) = \delta_{ij}$. So, the $\hat{e}_i$ are a dual basis over $A$ for the dual $R^*$ of $R$ with coefficients in $A$. Since the $\hat{e}_i$ are also a $F$-basis for the $F$-subspace $\hat{A} \equiv \{ \hat{a} \mid a \in A \}$ of $R^*$, $\hat{A}$ is an $F$-form of the $R$-module $R^*$ and $R^* \equiv \hat{A} \hat{A} = A \otimes_F A$. Endowing $R^*$ with the $A$-algebra product induced by the $F$-algebra product of $\hat{A}$ by ascent from $F$ to $A$, the identity and $A$-algebra product of $R^*$ are given by

$$1_{C^*} = 1_A, \quad \hat{a}\hat{b} = \hat{ab} \quad (a, b \in A).$$

Since the $A$-algebra $R^*$ has a finite $A$-basis, it induces a dual $A$-coalgebra structure on $R^*$ with coidentity $\varepsilon$ defined by

$$\varepsilon(x) \equiv x(1_A) \quad (x \in R)$$

and coproduct $\Delta(x) (x \in R)$ defined by the condition

$$\Delta(x) \equiv \sum_i x \otimes_A x_i \quad \Leftrightarrow \quad (\hat{a}\hat{b})(x) = \sum_i \hat{a}(i,x) \otimes_A \hat{b}(x_i) \quad (a, b \in A)$$

$$\Leftrightarrow \quad (\hat{a}\hat{b})(x) = \sum_i \hat{a}(i,x) \otimes_A \hat{b}(x_i) \quad (a, b \in A)$$

$$\Leftrightarrow \quad x(ab) = \sum_i x(a) \otimes_A x_i(b) \quad (a, b \in A).$$

This establishes that $R = \text{End}_F A$ is a preservation set—and, therefore, that $\text{End}_F A = \text{Pres}_F A$. □

**Definition 6.3.** A Galois biring of a commutative ring $A$ is a Galois ring $R$ of $A$ regarded as the biring $R = (\text{Pres}_A e, A, \pi, I_A, \Delta, \varepsilon)$ of preservations of $A$ over $F$ according to Theorem 6.1 and Definition 6.2.
For a coalgebra $C = (C, \Delta_C, \varepsilon_C)$ over $A$, the dual algebra $C^* = \text{Hom}_A(C, A)$ with coefficients in $A$ of $C$ is the $A$-module $C^* \equiv C^*(A)$ together with identity $1_C^* \equiv \varepsilon_C$ and algebra product $fg = \pi(f, g)$ defined by $$(fg)(x) \equiv \sum_i f(ix)g(xi) \quad (x \in C, \Delta_C(x) = \sum_i ix \otimes xi)$$ for $f, g \in C^*$. The following corollary is evident from the proof of Theorem 6.1.

**Corollary 6.1.** For a finite-dimensional commutative algebra $A/F$, the dual algebra $P^* = \text{Hom}_A(P, A)$ with coefficients in $A$ of the coalgebra $P \equiv \text{Pres}_F A$ over $A$ is the extension $\hat{A}A = A \otimes_F A$ of the $F$-algebra $A$ to $A$-algebra by ascent.

Theorem 6.1 establishes the Galois birings correspondence for a commutative ring $A$—the bijective Galois correspondence $F \leftrightarrow R \equiv \text{End}_F A, \; R \leftrightarrow F \equiv A^R$ between the subfields of $A$ of finite codimension and the Galois birings of $A$.

### 7. Galois descent

The Galois correspondence theorems for Galois objects (Galois groups, rings, Lie rings) $G$ acting on a field $K$ lead to Galois descent theorems—theorems which provide mechanisms of Galois descent from $K$-modules $V$ acted on by $G$ to $K^G$-modules $U = V^G$ [10,16,17]. This descent is inverse to Galois ascent $V = K \otimes_K U$ from $U$ to $V$ together with the corresponding action of the Galois object $G$ on $V$.

Now, more generally, the Galois correspondence theorems for Galois objects (Galois groups, rings, Lie rings, birings) $G$ acting on a commutative ring $A$ lead to Galois descent theorems providing mechanisms of Galois descent from $A$-modules $V$ acted on by $G$ to $A^G$-modules $U = V^G$. Again, this descent is inverse to Galois ascent $V = A \otimes_A U$ from $U$ to $V$ together with the corresponding action of the Galois object $G$ on $V$.

#### 7.1. Galois rings descent

Let $R$ be a Galois ring of $A$ with centralizer $F \equiv A^R$. Then Galois ring ascent by $R$ is the passage from an $F$-space $U$ to the $A$-module $V = A \otimes_F U$ regarded as $R$-module with respect to the action of $R$ on $V$ well defined by the condition $r(b \otimes u) \equiv r(b) \otimes u$ ($r \in R, b \in A, u \in U$). The resulting $V$ is an $R$-descent module with $R$-centralizer $V^R = 1 \otimes_F U$ in the following sense.

**Definition 7.1.** For a Galois ring $R$ of $A$, an $R$-descent module—or Galois rings descent module for $R$—is an $A$-module and (ring) $R$-module $V$ such that $(ar)v = a(rv)$
(r ∈ R, a ∈ A, v ∈ V). The centralizer of R in such a V is the \( A^R \)-submodule \( V^R = \{ u ∈ V \mid r(au) = r(a)u \ (r ∈ R, a ∈ A) \} \) of R in V.

The simplest instance of this is the Galois descent module \( V = A \)—whose \( A \)-module operation is the multiplication of \( A \) and whose \( R \)-module operation is the endomorphism ring action of \( R \) on \( A \).

The Jacobson endomorphism ring descent theorem \([10,16,17]\) generalizes from fields to commutative rings as follows—where \( A \) and \( R \) might come from any endomorphism ring \( S \) of a commutative algebra \( B \) which is finitely generated over \( B \)—as explained in Example 2.1.

**Theorem 7.1** (Galois rings descent theorem). Let \( V \) be an \( R \)-descent module for a Galois ring \( R \) of \( A \). Then \( V^R \) is a \( A^R \)-form of \( V \).

**Proof.** Let \( F \) be the field \( A^R \). By the Galois ring correspondence theorem, \( R = \text{End}_F A \). Take a basis \( e_1, \ldots, e_n \) for \( A \) over \( F \). Then \( a = \sum_j r_j(a) e_j \ (a ∈ A) \) where \( r_1, \ldots, r_n \) are the \( F \)-linear transformations from \( A \) to \( F \) such that \( r_j(e_k) = \delta_{jk} \ (1 ≤ i, j ≤ n) \)—the corresponding dual basis. Since the linear transformations \( E_{ij} = e_i r_j \) map \( e_k \) to \( \delta_{jk} e_i \) (\( 1 ≤ i, j, k ≤ n \)) they form a basis for \( R \) over \( F \). And the \( r_1, \ldots, r_n \) form a basis for \( R \) over \( A \)—with the unique linear combination delivering \( r ∈ R \) being \( r = \sum_j r(e_j)r_j \). Moreover, \( \sum_j E_{ij} = \sum_j e_j r_j \). Since \( r_j \) maps \( A \) into \( F \), then \( r(af)v = r(a)rv \) for \( r ∈ R, a ∈ A, 1 ≤ j ≤ n \). So then

\[
\begin{align*}
r(a(r_j v)) &= r((ar_j)v) = (r(ar_j))v = (r(a)r_j)v = r(a)(r_j v), \\
r(a(r_j v)) &= r(a)(r_j v)
\end{align*}
\]

for \( r ∈ R, a ∈ A, v ∈ V, 1 ≤ j ≤ n \). So, the \( r_j \) map the \( v ∈ V \) into \( V^R \), \( v = Iv = \sum_j e_j r_j v \) is in \( AV^R \), and \( V \) is the \( A \)-span of \( V^R \). To show that \( V^R \) is a \( F \)-form of \( V \), it remains only to show that \( F \)-independent elements \( v_k \) of \( V^R \) are \( A \)-independent. But an \( A \)-relation \( \sum_k f_k v_k = 0 \) leads to the \( F \)-relations \( \sum_k (r_j f_k) v_k = 0 \)—since the \( r_j \) map the \( f_k \) into \( F \). So, the \( r_j f_k \) are all 0. But then the \( f_k = \sum_j e_j r_j f_k \) are all 0. This establishes that the \( v_k \) are \( A \)-independent and \( V^R \) is an \( F \)-form of \( V \). \( \square \)

**Example 7.1.** Let \( B \) be a ring containing a commutative ring \( A \) as unital subring. Let \( R \) be a unital subring and finitely generated \( A \)-submodule of \( V = \text{End}_F A \) which stabilizes and acts faithfully and irreducibly on \( A \). Then \( R \) can be regarded as a Galois ring of \( A \)—and \( V \) as an \( R \)-descent module with \( R \)-action \( rv ∈ V \ (r ∈ R, v ∈ V) \). Then \( V^R \) is an \( R^F \)-form of \( V \) by Theorem 7.1.

**Example 7.2.** As an instance of Example 7.1, for a Galois ring \( R \) of \( A \) and \( F = A^R \), \( V = \text{End}_F A \) is an \( R \)-descent submodule of \( \text{End} A \). Its centralizer is the dual space

\[ V^R = \text{Hom}_F(A, A)^R = \text{Hom}_F(A, A^R) = \text{Hom}_F(A, F) = A^* \]
of $A$ over $F$. In this instance, Theorem 7.1 simply reconfirms that $A^*$ is an $F$-form of $\text{End}_F A$.

7.2. Galois groups descent

Let $G$ be a Galois group of $A$ with centralizer $F \equiv A^G$. Then Galois group ascent by $G$ is the passage from an $F$-space $U$ to the $A$-module $V \equiv A \otimes_F U$ regarded as $G$-module with respect to the action of $G$ on $V$ well defined by the condition $g(b \otimes u) \equiv g(b) \otimes u$ ($g \in G, b \in A, u \in U$). The resulting $V$ is a $G$-descent module with $G$-centralizer $V^G \equiv 1 \otimes_F U$ in the following sense.

**Definition 7.2.** For $G$ a Galois group of $A$, a $G$-descent module—or Galois groups descent module for $G$ on $A$—is an $A$-module and (group) $G$-module $V$ such that $a(g)v \equiv g(a)v$ ($g \in G, a \in A, v \in V$) and $\sum_{g \in G} a_g v = 0 \Rightarrow \sum_{g \in G} a_g g = 0$ ($g \in G, a_g \in A$) where $g$ is the linear transformation of $V$ defined by $g(v) \equiv gv$ ($g \in G, v \in V$). The centralizer of $G$ in such a $V$ is the $A^G$-submodule $V^G \equiv \{u \in V \mid g(u) = u$ ($g \in G)\}$ of $G$ in $V$.

The simplest instance of this is the Galois groups descent module $V = A$ for $G$ on $A$—whose $A$-module operation is the multiplication of $A$ and whose $G$-module operation is the automorphism group action of $G$ on $A$.

**Remark 7.1.** The condition

$$\sum_{g \in G} a_g g = 0 \Rightarrow \sum_{g \in G} a_g g = 0 \quad (g \in G, a_g \in A)$$

is the nondegeneracy condition. It is satisfied automatically when $A$ is a field—in which case

$$\sum_{g \in G} a_g g = 0 \Rightarrow a_g = 0 \quad (g \in G, a_g \in A)$$

by Dedekind’s lemma on the linear independence of the $g \in G$ over $A$. When $A$ is not a field, the $g \in G$ are usually not linearly independent.

The descent theorem of A. Speiser [16, Theorem 3.2.5] generalizes from fields to commutative rings as follows—where $A$ and $G$ might come from any finite group $H$ of automorphisms of any commutative algebra $B$ as described in Example 3.1.

**Theorem 7.2** (Galois groups descent theorem). Let $V$ be a $G$-descent module for a finite-irreducible automorphism group $G$ of $A$. Then $V^G$ is an $A^G$-form of $V$.

**Proof.** Let $R$ be the span of $G$ over $A$. Then $R$ is a Galois ring of $A$ since $G$ is finite-irreducible and $(ag)(bh) = ag(b)gh$ ($a, b \in A; g, h \in G$). The nondegeneracy condition
\[ \sum_{g \in G} a_g g = 0 \Rightarrow \sum_{g \in G} a_g g_{\lambda} = 0 \quad (g \in G, a_g \in A) \]
ensures that the action of \( G \) on \( V \) extends to an action of \( \mathbb{R} \) on \( V \) relative to which \( V \) is an \( R \)-descent module. By Theorem 7.1, \( V^R \) is then a \( V^R \)-form of \( V \). This completes the proof, since \( A^G = A^R \) and \( V^G = V^R \)—as shown by the following computations:

\[
\begin{align*}
u \in V^R & \Rightarrow g(u) = g(1) = 1 \cdot u \quad (g \in G) \Rightarrow u \in V^G, \\u \in V^G & \Rightarrow g(au) = g(a)g(u) = g(a)u \quad (a \in A, g \in G) \Rightarrow u \in V^R.
\end{align*}
\]

**Example 7.3.** For \( G \) a finite-irreducible automorphism group of \( A \), the \( A \)-module \( V \equiv \operatorname{End} A \) is a \( G \)-descent module with \( G \)-module action

\[
g(v)(b) \equiv gv^{-1}b \quad (a, b \in A, \ g \in G, \ v \in V).
\]

In fact, the descent condition \( g(av) = g(a)g(v) \) is established as follows:

\[
g(av)(b) = g(av)g^{-1}b = g\{a\{v(g^{-1}b)\}\} = g(a)g\{v(g^{-1}b)\} = g(a)gv^{-1}b = (g(a)g(v))(b).
\]

Its centralizer

\[
V^G = (\operatorname{End} A)^G = \{ v \in \operatorname{End} A \mid g(v) = v \ (g \in G) \}
\]

is an \( A^G \)-form of \( \operatorname{End} A \) by Theorem 7.2.

**Example 7.4.** As an instance of Example 7.3, suppose that \( A = F^n \) is the direct sum of \( n \) copies of \( F \) and \( P \) is the symmetric group on \( n \) letters acting as a group of automorphisms of \( A \) over the diagonal \( \overline{F} \) and permuting the \( F \) factors in the manner of Corollary 3.1 part 4. Then \( (\operatorname{End}_{\overline{F}} A)^F \) is an \( F \)-form of \( \operatorname{End} A \).

**Example 7.5.** For \( G \) a finite-irreducible automorphism group of \( A \) and \( F \equiv A^G \), \( \operatorname{Der}_F A \) is a \( G \)-descent submodule of the \( G \)-descent module \( \operatorname{End} A \) of Example 7.3. By Theorem 7.2, its centralizer \( (\operatorname{Der}_F A)^G \) is an \( F \)-form of \( \operatorname{Der}_F A \).

### 7.3. Galois Lie rings descent

Let \( D \) be a Galois Lie ring of \( A \) with centralizer \( F \equiv A^D \). Then Galois Lie ring ascent by \( D \) is the passage from an \( F \)-space \( U \) to the \( A \)-module \( V \equiv A \otimes_F U \) regarded as \( D \)-module with respect to the action of \( D \) on \( V \) well defined by the condition \( d(b \otimes u) \equiv d(b) \otimes u \ (d \in D, b \in A, u \in U) \). The resulting \( V \) is a \( D \)-descent module with \( D \)-centralizer \( V^D = 1 \otimes_F U \) in the following sense.

Definition 7.3. A D-descent module—or Galois Lie rings descent module for D on A—is an A-module and (Lie ring) D-module V such that \((ad)v = a(dv), d(av) = d(a)v + a(dv),\) and \((d_a)^p = d_a^p (d \in D, a \in A, v \in V)—where \(d_a\) is the linear transformation \(d_a(v) \equiv dv (v \in V)\) of V. The centralizer of D in such a V is the \(A^D\)-submodule

\[
V^D \equiv \{u \in V \mid d(a)u = a(d)u (d \in D, a \in A)\} = \{u \in V \mid d(u) = 0 (d \in D)\}
\]
of D in V.

The condition \((d_a)^p = d_a^p (d \in D, a \in A, v \in V)\) is simply the condition that the Lie ring D-module V be restricted.

The simplest instance of this is the Galois Lie rings descent module \(V = A\) for D on A—whose A-module operation is the multiplication of A and whose D-module operation is the derivation ring action of D on A.

Definition 7.4. A toral form of a Galois Lie ring D is a commutative \(A^D\)-Lie subalgebra of D such that \(T_\pi \equiv \{t \in T \mid t^p = t\}\) is a \(\pi\)-form of D where \(\pi = \{0, \ldots, p - 1\}\) is the prime field of F.

The \(T_\pi\) of a toral form T of a Galois Lie ring D is a \(\pi\)-form \(T_\pi\) of T called the prime form of T. Since T is abelian with restricted prime form, T itself is restricted.

Theorem 7.3. Let D be a Galois Lie ring D of A. Then D has a dual generating system \(d_1, \ldots, d_m \in D, e_1, \ldots, e_m \in A\) such that \(T = F e_1 d_1 + \cdots + F e_m d_m\) is a toral form of D.

Proof. Let F be the field \(A^D\) and take a dual generating system \(d_1, \ldots, d_m \in D, e_1, \ldots, e_m \in A\) for D. If \(e_i\) is nilpotent, since \(e_i^p\) is in F, it is 0—so that \((e_i + 1)^p = 0 + 1 = 1\). Since derivations vanish at 1, replacing the nilpotent \(e_i\) by \(e_i + 1\) then results in a dual generating system \(d_1, \ldots, d_m \in D, e_1, \ldots, e_m \in A\) for D where the \(e_i^p\) are nonzero elements of F. The \(e_i\) are then invertible with inverse \(e_i^{-1} = (e_i^p)^{-1}\). By Theorem 5.1, \(L = F d_1 + \cdots + F d_m\) is a derivation ring form of A and F-form of D. Let \(t_i \equiv e_i d_i\) (\(1 \leq i \leq m\)) and \(T \equiv F t_1 + \cdots + F t_m\). Since the \(e_i\) are invertible, \(D = A L = A T = A T_\pi\).

So, T is also an F-form of D—and \(T_\pi \equiv \pi t_1 + \cdots + \pi t_m\) is a \(\pi\)-form of D. Furthermore, \(T\) and \(T_\pi\) are restricted abelian Lie subrings of D. In fact, the evident equalities

\[
t_i t_j (e_k) = t_i (\delta_{jk} e_k) = \delta_{ik} (\delta_{jk} e_k) = \delta_{jk} (\delta_{ik} e_k) = t_j (\delta_{ik} e_k) = t_j t_i (e_k),
\]

\[
t_i^p (e_k) = t_i (e_k)
\]

for \(1 \leq i, j, k \leq m\) lead to the equalities

\[
t_i t_j = t_j t_i, \quad t_i^p = t_i
\]

for \(1 \leq i, j \leq m\) since the \(e_k (1 \leq k \leq m)\) separate the elements of D. These identities also show that \(T_\pi = \{t \in T \mid t^p = t\}\)—since the coefficients \(a_i \in F\) of any \(a_1 t_1 + \cdots + a_m t_m \in T\) such that
\[ a_1^p t_1 + \cdots + a_m^p t_m = (a_1 t_1 + \cdots + a_m t_m)^p = a_1^p t_1 + \cdots + a_m^p t_m \]
satisfy the condition \( a_i^p = a_i \) and so are in the splitting field \( \pi \) of the polynomial \( X^p - X \). So, \( T \) is a toral form of \( D \). \( \square \)

The Jacobson differential descent theorem [10,16] generalizes from fields to commutative rings as the following Theorem 7.4—where \( A \) and \( D \) might come from any finitely generated derivation ring \( E \) of any commutative algebra \( B \) as described in Example 4.1.

The proof of Theorem 7.4, motivated by that of the corresponding [16, Theorem 5.2.9] for fields, illustrates how toral forms \( T \) of Galois Lie rings \( D \) are used. The irreducibility of \( D \) on \( A \) makes up for the absence of inverses when the fields \( K \) of [16] are now generalized to commutative rings \( A \).

**Theorem 7.4** (Galois Lie rings descent theorem). Let \( V \) be a \( D \)-descent module for a Galois Lie ring \( D \) of \( A \). Then \( V^D \) is an \( A^D \)-form of \( V \).

**Proof.** Let \( F = A^D \), let \( T \) be a toral form of \( D \), and let \( T_\pi = \pi t_1 + \cdots + \pi t_m \) be its prime form—the \( t_i \) being a basis for \( T_\pi \) over \( \pi \). Since \( t^p = t \) for \( t \in T_\pi \), and since \( V \) is a restricted Lie module for \( T \), \( t^p = t \) and the separable polynomial \( X^p - X \) vanishes on the \( t_i \in T_\pi \) acting on the \( \pi \)-space \( V \). So, the eigenvalues of the \( t_i \in T_\pi \) are in the splitting field \( \pi \) of \( X^p - X \) and the \( t_i \in T_\pi \) act diagonalizably on \( V \). Since \( T_\pi \) is abelian, \( V \) has spectral decomposition \( V = \sum_{\sigma \in S} V_\sigma \) where \( S \) is the set of \( \sigma \) in the \( \pi \)-dual space \( T_\pi^* \) of \( T_\pi \) for which \( V_\sigma = \{ v \in V \mid tv = \sigma(t)v \} \) is nonzero.

Applying this to the special case where the Galois descent module is \( A \), \( A \) too has spectral decomposition \( A = \sum_{\alpha \in R} A_\alpha \) where \( R \) is the set of \( \alpha \) in the \( \pi \)-dual space \( T_\pi^* \) of \( T_\pi \) for which \( A_\alpha = \{ t \in A \mid \pi t = \alpha(t) \pi \} \) is nonzero.

The first part of the proof is to show that the spectral decompositions \( A = \sum_{\alpha \in R} A_\alpha \) and \( V = \sum_{\sigma \in S} V_\sigma \) are \( A = \sum_{\alpha \in R} A_\alpha A_\beta = \sum_{\alpha \in R} F x_\alpha \) and \( V = \sum_{\sigma \in S} x_\sigma V_\sigma \).

Taking nonzero \( x_\alpha \in A_\alpha \) \( (\alpha \in R) \), \( x_\alpha A = A \) for \( \alpha \in R \). To see this, note that \( x_\alpha \) is stable under all \( t \in T_\pi \) by the computation

\[ t(x_\alpha b) = t(x_\alpha) b + x_\alpha t(b) = \alpha(t) x_\alpha b + x_\alpha t(b) \in x_\alpha A \]

for \( b \in A \). But then \( x_\alpha \) is also stable under \( D \)—since \( D = AT_\pi \) and

\[ (at)(x_\alpha A) = a \big( t(x_\alpha A) \big) \subseteq a(x_\alpha A) \subseteq x_\alpha A \]

for \( a \in A, t \in T_\pi \). Since \( D \) is irreducible on \( A \), it follows that \( x_\alpha A = A \) \( (\alpha \in R) \).

From \( A = \sum_{\alpha \in R} A_\alpha, A_\alpha A_\beta = A_{\alpha+\beta} \) \( (\alpha, \beta \in R) \), and \( x_\alpha A = A \) \( (\alpha \in R) \) come the inclusions

\[ \sum_{\gamma \in R} A_{\gamma} = A = x_\alpha A = \sum_{\beta \in R} x_\alpha A_\beta \subseteq \sum_{\beta \in R} A_{\alpha+\beta}. \]
Evidently, then, the \( x_{\alpha}A_{\beta} \) are nonzero and \( x_{\alpha}A_{\beta} = A_{\alpha + \beta} \) for all \( \alpha, \beta \in R \). Consequently, \( \alpha + \beta \) is nonzero and \( \alpha + \beta \in R \) for all \( \alpha, \beta \in R \). Since \( R \) is an additively closed subset of the finite additive group \( T^*_\pi \), \( R \) is an additive subgroup of \( T^*_\pi \). Since \( \pi \) is the prime field of \( p \) elements, the subgroup \( R \) of the \( \pi - \text{space} \) \( T^*_\pi \) is a \( \pi - \text{subspace} \) of \( T^*_\pi \). Finally, since \( R \) separates the points of \( T^*_\pi \), the \( \pi - \text{subspace} \) \( R \) of \( T^*_\pi \) is \( R = T^*_\pi \).

Taking \( \beta = 0 \) in \( x_{\alpha}A_{\beta} = A_{\alpha + \beta} \) gives

\[
A_\alpha = A_{\alpha + 0} = x_\alpha A_0 = x_\alpha F = Fx_\alpha.
\]

So, \( A_\alpha = Fx_\alpha \) for \( \alpha \in R \) and \( A = \sum_{\sigma \in S} Fx_\sigma \).

Since \( x_\alpha A = A \), \( x_\alpha V \supseteq x_\alpha AV = AV = V \) and \( x_\alpha V = V \) (\( \alpha \in R \))—from which come the inclusions

\[
\sum_{\gamma \in S} V_\gamma = V = x_\alpha V = \sum_{\sigma \in S} x_\alpha V_\sigma \subseteq \sum_{\sigma \in S} V_{\alpha + \sigma}.
\]

Evidently, then, the \( x_\alpha V_\sigma \) are nonzero and \( x_\alpha V_\sigma = V_{\alpha + \sigma} \) for all \( \alpha, \sigma \in S \). For \( \sigma \in S \), then, \( V_{\alpha + \sigma} \) is nonzero and \( \alpha + \sigma \in S \) for all \( \alpha \in R \). Since \( R = T^*_\pi \), it follows that \( R + \sigma \subseteq S \subseteq R \). Since \( R + \sigma \) and \( R \) are finite with the same number of elements, it follows that \( R + \sigma = S = R \), that is, \( S = R = T^*_\pi \).

The point of all this is that, since \( S = T^*_\pi \), \( S \) contains 0—and then, upon taking \( \sigma = 0 \) in the equation \( x_\alpha V_\sigma = V_{\alpha + \sigma} \), that

\[
V_\alpha = V_{\alpha + 0} = x_\alpha V_0.
\]

This establishes that \( V_\alpha = x_\alpha V_0 \) for \( \alpha \in R \) and \( V = \sum_{\alpha \in R} x_\alpha V_0 \)—completing the first part of the proof.

Proving that \( V^D = V_0 \) is an \( F \)-form of \( V \) reduces to showing that the bilinear pairing \( a, u \mapsto au \) (\( a \in A \), \( u \in V_0 \)) from \( A \), \( V_0 \) to \( V \) is a tensor product \( V = A \otimes F \, V_0 \). By the first part of the proof, the span of the image of this pairing is

\[
AV_0 = \left( \sum_{\alpha \in R} Fx_\alpha \right) V_0 = \sum_{\alpha \in R} x_\alpha V_0 = \sum_{\alpha \in R} V_\alpha = V.
\]

So, it remains only to show that \( A \) and \( V_0 \) are linearly-disjoint over \( F \), that is, \( F \)-linearly independent elements of \( V_0 \) are \( A \)-linearly independent.

Suppose, to the contrary, that \( A \) and \( V_0 \) are not linearly-disjoint over \( F \) and choose a set of linearly independent \( u_1, \ldots, u_n \) with \( n \) minimal for which there exist relations \( a_1 u_1 + \cdots + a_n u_n = 0 \) over \( A \) (with the \( a_i \) being from \( A \)) with not all 0. By the minimality of \( n \), all these \( a_i \) are nonzero—including \( a_1 \). Consequently, the set \( J \) of all \( a_1 \in A \) for which there is a relation \( a_1 u_1 + \cdots + a_n u_n = 0 \) over \( A \) is then a nonzero ideal of \( A \).

Since the \( d \in D \) satisfy \( d(u) = 0 \) (\( u \in V_0 \)), a relation \( a_1 u_1 + \cdots + a_n u_n = 0 \) over \( A \) leads to corresponding relations \( a(\alpha_1) u_1 + \cdots + a(\alpha_n) u_n = 0 \) (\( d \in D \)) over \( A \)—from which it follows that \( J \) is a nonzero \( D \)-stable ideal of \( A \). Since \( D \) is irreducible on \( A, J = A \).

So, \( J \) contains 1 and there exists a relation \( a_1 u_1 + \cdots + a_n u_n = 0 \) over \( A \) with \( a_1 = 1 \). But then
\[ d(a_1) = d(1) = 0. \] So, the relation \( a_1 u_1 + \cdots + a_n u_n = 0 \) leads to the corresponding shorter relations \( d(a_2) u_2 + \cdots + d(a_n) u_n = 0 \) (\( d \in D \)). By the minimality of \( n \), the coefficients \( d(a_i) \) (\( d \in D \)) are then all 0—and \( a_1, \ldots, a_n \in A^D = F \). Since the \( a_i \) are not all zero, this contradicts the linear independence of the \( u_i \) over \( F \). Retreating from the supposition to the contrary, \( A \) and \( V_0 \) then are linearly-disjoint over \( F \). □

**Example 7.6.** Let \( V \) be a ring containing a commutative ring \( A \) as unital subring—and regard \( V \) as \( A \)-module. Let \( D \) be an \( A \)-submodule and restricted Lie subalgebra of \( \text{Der} A V \) which stabilizes and acts irreducibly on \( A \) with the field \( F \equiv A^D \) finite-codimensional—and suppose that restriction of \( D \) to \( A \) is faithful. Then \( D \) may be regarded as a Galois Lie ring of \( A \)—and \( V \) as a \( D \)-descent module. So, its centralizer

\[
V^D = \{ v \in V \mid x(av) = x(a)v \ (a \in A, \ x \in D) \} = \{ v \in V \mid x(v) = 0 \ (x \in D) \}
\]

is an \( F \)-form of \( V \) by Theorem 7.4.

### 7.4. Galois birings descent

The Galois birings descent theorem is an important footnote to the Galois rings descent theorem—for the following reasons:

1. Moving from Galois rings theory of Section 2 to the Galois birings theory of Section 6 amounted largely to endowing Galois rings with biring structures—so that the structure of the ring extension \( A/F \) and the structure of the corresponding biring \( \text{Pres}_F A \) faithfully reflect each other.
2. Galois biring ascent changes in name only. And, accordingly, Galois birings descent changes in name only.
3. Importantly, however, the nature of the underlying action for a Galois biring can be described in terms of the nature of the biring, as explained in Theorem 7.5.
4. This enables it to be shown—in Corollaries 7.1 and 7.2—that a Galois ring descent module \( V \) for the Galois ring \( AG \) (respectively \( A(D) \)) generated by a Galois group \( G \) (respectively Lie ring \( D \)) is, in fact, a Galois group (respectively Lie ring) descent module for \( G \) (respectively \( D \)).

Let \( R \) be a Galois biring of \( A \) with centralizer \( F \equiv A^R \). Then \( \text{Galois biring ascent} \) by \( R \) is simply Galois ring ascent by \( R \)—the passage from an \( F \)-space \( U \) to the \( A \)-module \( V \equiv A \otimes_F U \) regarded as \( R \)-module with respect to the action of \( R \) on \( V \) well defined by the condition \( r(b \otimes u) = r(b) \otimes u \ (r \in R, b \in A, u \in U) \). The resulting \( V \) is then an \( R \)-descent module with \( R \)-centralizer \( V^R = 1 \otimes_F U \) in the following sense.

**Definition 7.5.** An \( R \)-descent module—or Galois birings descent module for \( R \) on \( A \)—is simply an \( A \)-descent module for \( R \) as Galois ring of \( A \). And the centralizer of \( R \) in such a \( V \) is the centralizer \( V^R \) in \( V \) of \( R \) as Galois ring of \( A \).
The simplest instance of this is the Galois birings descent module $V = A$ for the Galois biring $R$ of $A$—whose $A$-module operation again is the multiplication of $A$ and whose $R$-module operation is the endomorphism ring action of $R$ on $A$.

The Galois rings descent Theorem 7.1 leads at once to the following theorem.

**Theorem 7.5** (Galois birings descent theorem). Let $V$ be an $R$-descent module for a Galois biring $R$ of $A$. Then

1. $V^R$ is a $A^R$-form of $V$.
2. $x(ay) = \sum_i x(a)x_i y$ ($x, y \in R$, $\Delta(x) = \sum_i x \otimes_A x_i$).

**Proof.** That $V^R$ is an $A^R$-form of $V$ is the content of Theorem 7.1—which establishes (1).

For (2), letting $U = V^R$, it suffices to prove

$$x(ay) = \sum_i x(a)x_i y$$

for $x, y \in R$, $\Delta(x) = \sum_i x \otimes_A x_i$, and $v = bu$ ($b \in A$, $u \in U$). This, in turn, is evident from the equations

$$x(ay) = x((ab)u) = (\sum_i x(a)x_i (b))u = \sum_i x(a)x_i (bu) = \sum_i x(a)x_i (v)$$

for $x, y \in R$, $\Delta(x) = \sum_i x \otimes_A x_i$. □

**Example 7.7.** For $R$ a Galois biring of $A$ and $F = A^R$, $V = \text{End}_F A$ as $A$-module is an $R$-descent module with respect to the $R$-module action $(rv)(b) = r(v(b))$ ($a, b \in A$, $r \in R$, $v \in V$). As in Example 7.2, its centralizer is the dual space $V^R = \text{Hom}_F (A, F) = A^*$ of $A$ over $F$. The formula

$$x(ay) = \sum_i x(a)x_i y \quad (x, y \in R, \Delta(x) = \sum_i x \otimes_A x_i)$$

follows from the second part of Theorem 7.5.

**Corollary 7.1.** Let $G$ be a Galois group of $A$ and $V$ a Galois rings descent module for the $A$-span $A^G$ of $G$. Then $V$ is a $G$-descent module for $A$.

**Proof.** Since $G$ consists of automorphisms of $A$, $\Delta(g) = g \otimes_A g$ ($g \in G$). But then

$$g(ay) = g(a)gv \quad (g \in G, a \in A, v \in V)$$

by Theorem 7.5. Since $V$ is an $A^G$-module, the nondegeneracy condition is satisfied. □
Corollary 7.2. Let $D$ be a Galois Lie ring of $A$ and $V$ a Galois rings descent module for the $A$-span $A(D)$ of the enveloping ring $(G)$ of $G$. Then $V$ is a $D$-descent module for $A$.

Proof. Since $D$ consists of derivations of $A$, $\Delta(x) = x \otimes A e + e \otimes A x$ ($x \in D$)—where $e \equiv I_A$. But then
\[ x(av) = x(a)v + axv \quad (x \in D, \ a \in A, \ v \in V) \]
by Theorem 7.5. □

8. The simple derivation ring problem

A Lie ring $D$ is simple when $[D, D] \neq 0$ and $D$ has no ideals other than 0 and $D$. When $D$ is a simple Lie ring, its centroid $F$ (centralizer of $ad D$ in $End D$) is a field—since $D = [D, D]$. So, $D$ may be regarded as a Lie algebra over $F$.

In Definitions 4.1 and 4.2, a derivation ring is a Lie subring $D$ of the Lie ring $Der(A)$ of derivations of some commutative ring $A$ such that $AD \subseteq D$; and when some such $A$ is $D$-simple, $D$ is an irreducible derivation ring.

This section formulates four successively easier problems concerned with determining simple derivation rings.

Problem 8.1 (Simple derivation rings problem). Determine all simple derivation rings.

Any simple Lie ring $D$ with centralizer $F$ has a faithful module $V$ over $F$—such as its adjoint module $D$ (which is faithful by the simplicity of $D$). Corresponding to any such $V$ is its augmentation module algebra—the $D$-module $A \equiv F \oplus V$ with $DF = 0$ regarded as commutative algebra over $F$ with $V$ being a maximal ideal of $A$ with $VV = 0$. Imbedding $D$ in $Der(A)$ by way of its module action on $A$, $D$ is then a simple derivation ring of $A$.

This proves the following theorem.

Theorem 8.1. The problem of determining all simple Lie rings is equivalent to the simple derivation ring problem, Problem 8.1.

Problem 8.1 becomes more tractable when a nondegeneracy condition is imposed which excludes derivation rings $D$ of their augmented module algebras.

Definition 8.1. A derivation ring $D$ of $A$ is nondegenerate if its induced action on $A/M$ is nonzero for every maximal ideal $M$ of $A$ which is stable under $D$. A nondegenerate derivation ring is a nondegenerate derivation ring of some $A$.

Problem 8.2 (Simple nondegenerate derivation rings problem). Determine all simple nondegenerate derivation rings.

Theorem 8.2. A simple nondegenerate derivation ring is an irreducible derivation ring.
**Proof.** Let \( D \) be a simple nondegenerate derivation ring of \( A \) and let \( M \) be a maximal \( D \)-stable ideal of \( A \) different from \( A \). Since \( A \) is unital, such an \( M \) exists by Zorn’s lemma.

Suppose that \( DA \subseteq M \). Then \( M + Aa \) is a \( D \)-stable ideal of \( A \) for \( a \in A \). So, by the maximality of \( M \) as \( D \)-stable ideal, \( M + Aa = A \) for all \( a \in A - M \), that is, \( M \) is a maximal ideal of \( A \). But the maximal ideal \( M \) of \( A \) is \( D \)-stable and the action of \( D \) on \( A/M \) is zero—contradicting the assumption that \( D \) is a nondegenerate derivation ring of \( A \). This rules out \( DA \subseteq M \).

Having ruled out \( DA \subseteq M \), \( D \) is an irreducible derivation ring of \( A \). After all, \( D \neq 0 \), the representation of \( D \) on \( A \) is faithful—since \( D \) is simple and \( DA \neq 0 \); and 0, \( A \) are the only \( D \)-stable ideals of \( A \) by the choice of \( M \). So, \( D \) is an irreducible derivation ring in the sense of Definition 4.2. \( \square \)

Theorem 8.2 reduces the simple nondegenerate derivation ring problem to the following problem.

**Problem 8.3 (Simple irreducible derivation rings problem).** Determine all simple irreducible derivation rings.

One direction of Problem 8.3 is solved by the following remarkably general theorem of [11]. This theorem establishes that all irreducible derivation rings are simple as Lie algebras except those of characteristic 2 which are cyclic and not “surjective.”

**Theorem 8.3 (Jordan [11]).** Let \( D \) be a nonzero \( A \)-submodule and Lie subring of \( \text{Der}(A) \) which stabilizes no ideals of \( A \) other than 0 and \( A \). Then \( D \) is simple as Lie algebra except possibly when the characteristic is 2 and \( D \) is cyclic as \( A \)-module. When the characteristic is 2 and \( D = Ad \), then \( D \) is a simple Lie algebra if and only if \( d(A) = A \).

Theorem 8.3 reduces solving Problem 8.3 to determining all irreducible derivation rings. One approach to doing so, begun in [20], is based on the central simple theory for algebras with operators [18]. Structure theorems [20, 7.3, 7.4] for central simple Jordan Lie algebras and their modules are the key to the determining all simple locally nilpotent separably triangulable unital Lie algebras. Classification of their closures—the simple Jordan Lie algebras—then reduces to classifying those which are nil and toral. And classification of their absolutely irreducible modules reduces to classifying those which are toral. In particular, [20, 7.3, 7.4] make tractable the problem of classifying all simple Lie algebras of Witt type—over arbitrary fields up to purely inseparable descent.

Problem 8.3 becomes more tractable upon imposing the condition that \( D \) be restricted.

**Problem 8.4 (Simple restricted irreducible derivation rings problem).** Determine all simple restricted irreducible derivation rings.

By Theorems 4.2 and 8.3, Problem 8.4 is solved in the finitely generated case as follows.

**Theorem 8.4.** A finitely generated restricted irreducible derivation ring \( D \) is the derivation algebra \( \text{Der}_F A \) of some finite-dimensional truncated polynomial algebra \( A \) over the
centroid $F$ of $D$. It is simple if and only if the characteristic is not 2 or the characteristic is 2 and $A$ is not of the form $A = F \oplus Fa$ with $a^2 \in F$.

Acknowledgments

This paper has benefited particularly from conversations with Bruce Allison, John Faulkner, and Kevin McCrimmon following a talk on part of it given at the University of Virginia; from the efforts, thoughtful queries, shared insights, and suggestions of Michel Van den Bergh and the reviewer; and from the referenced work of Richard Block and David Jordan. It is a pleasure to thank them all at this time.

References