Universidad Autónoma de Madrid | Escuela de Doctorado

Purely inseparable extensions of rings

Celia del Buey de Andrés

Director: Orlando E. Villamayor Uriburu

Programa de Doctorado en Matemáticas
Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

Madrid, 2024

Al yayo Jaime,
para que encuentre la aplicación a las quinielas.

Agradecimientos

Dar gracias consiste en reconocer todo aquello que se nos regala, tomar conciencia de la fortuna que nos supone y manifestarlo para dejar constancia de ello. En este punto del trayecto, dar gracias no deja de ser un ejercicio necesario, aunque posiblemente no sea suficiente con las líneas que siguen a continuación.

Gracias, Orlando, por tu dedicación y tu confianza en estos años, por acompañar mi aprendizaje con nuevas preguntas y desafíos, y por compartir generosamente tu visión de las matemáticas conmigo. También gracias, Diego, por el trabajo compartido en este proceso y por ofrecerme siempre tantas oportunidades como sugerencias.

Gracias al grupo de investigación de geometría algebraica y aritmética por recibirme y contar conmigo como una más. En particular, gracias, Ana, por seguir despertando mi inquietud matemática y por las facilidades que has dispuesto para que llegase hasta aquí. Gracias, Adolfo, por tus buenos consejos y tu disponibilidad siempre que lo he necesitado. Gracias, Santi, por valorar y leer cuidadosamente esta tesis. Gracias, Angélica, por tu buen ánimo y tu sabiduría popular. Gracias a todos los que formáis parte del equipo por vuestra ayuda en estos años.

De manera más amplia, gracias a quienes han hecho valiosa mi estancia en el Departamento de Matemáticas. Gracias a quienes ya estaban cuando yo llegué: Luis, Adri, Jan, Julio, Álex, Diego, Jaime, Fran y Manuel, por acogerme con cuidado, generosidad y buen humor. Gracias a quienes habitaron mucho antes el despacho haciendo que ahora sea un lugar de curiosas reliquias y algunas plantas que le dan algo más de vida. Gracias a quienes llegaron al mismo tiempo: Ismael y Mikel, por ser ejemplo de que es posible. Gracias a todos los profesores, ahora ya compañeros, que no han dejado de alentar mi interés por las matemáticas. Gracias a quienes llegaron después, por su entusiasmo y su ánimo para continuar el legado: Edu, Irene, Peio, Henrique, Jorge, Itahisa, Javi, Jorge, Sergio, Teresa, David, Victoria, Esther, Alicia...

Y el último agradecimiento es con la Vida que se manifiesta en las personas que la convierten en regalo. Gracias, papá y mamá, por concedérmela, transmitírmela y enseñarme a vivirla. Gracias, Natalia, por disfrutarla conmigo a cada momento. En lo que falta, no alcanza para tantos nombres, pero seguro todos serán capaces de reconocerse en alguna de las siguientes líneas. Gracias a quienes con amor me acompañan a cada paso. Gracias a quienes están sin importar las condiciones. Gracias también a quienes ya se fueron, pero siguen estando de otra manera. Gracias a quienes con sus pasos me señalan el camino. Gracias a quienes me ayudan a sostenerme en mis principios. Gracias a quienes me animan permanecer en búsqueda. Gracias a quienes me impulsan para alcanzar plenitud. En definitiva, gracias a todos ellos por hacer que el camino adquiera sentido.

Contents

Introducción **v**

Introduction **xvii**

1 On projective modules **1**

1.1 Preliminaries on projective modules 2
1.2 Projective ring extensions 6
1.3 Generalization of the Jacobson-Bourbaki Theorem 8
1.4 Grassmannian of subalgebras 15

2 Purely inseparable Galois extensions of exponent one **19**

2.1 Preliminaries for Galois extensions 21
2.1.1 Exponent of a ring extension 21
2.1.2 Derivations and Kähler differentials 25
2.1.3 On p-basis 28
2.1.4 Differentiably simple rings 30
2.2 Galois extensions of rings 36
2.2.1 Galois extensions and differentiably simple rings 37
2.2.2 Galois extensions and the module of differentials 39
2.2.3 Galois extensions and derivations 42
2.2.4 Summary of characterizations of Galois extensions 48
2.3 Towers of Galois extensions 50
2.3.1 Basics on Galois towers of rings 50
2.3.2 Preliminaries on affine group schemes 52
2.3.3 Automorphism group scheme of an extension with splitting p-basis 55
2.3.4 Yuan scheme 58

3 Purely inseparable extensions of higher exponent **63**

3.1 Purely inseparable extensions of rings as special algebras 65
3.1.1 (Generalized) normal generating sequences 65
3.1.2 On purely inseparable extensions of rings 68
3.2 Purely inseparable extensions of rings and differential operators 74
3.2.1 Differential operators and modules of principal parts 75
3.2.2 Extension of differential operators along Galois extensions . . . 80
3.2.3 Purely inseparable extensions, differential operators and modules of principal parts 87
3.3 Towers of purely inseparable extensions 94
3.3.1 Intermediate subrings of a purely inseparable ring extension . . 95
3.3.2 Composition of purely inseparable extensions of rings 99

4 Modular extensions of rings **103**
4.1 Preliminaries for modular extensions 104
4.1.1 Linearly disjointedness 104
4.1.2 Generalized p-generating sequences 107
4.1.3 Generalized p-basis 110
4.2 On modular extensions of rings 114
4.2.1 Basics on modular extensions 115
4.2.2 Modular extensions and linearly disjointedness 116
A Commutative algebra **121**
A.1 Some concepts of rings 121
A.2 Some properties of modules 122
A.3 Some properties of algebras 129
Bibliography **135**

Introducción

Las extensiones de cuerpos puramente inseparables son un objeto de especial interés para el Álgebra Conmutativa. Han sido estudiadas ampliamente, en particular, con vistas a desarrollar un análogo de la teoría de Galois clásica establecida para extensiones separables de cuerpos. El principal objetivo de esta tesis es estudiar la extensión de esta noción de extensiones puramente inseparables al caso de extensiones de anillos y generalizar algunas de las propiedades y resultados que se conocen para extensiones de cuerpos puramente inseparables a este contexto más amplio.

Palabras clave: Extensiones puramente inseparables de anillos, torres de anillos, operadores diferenciales, p-bases, módulos proyectivos, extensiones modulares.

Códigos de clasificación MSC: 13B05, 13N10, 13C10, 14M15, 14L17

Motivación

En lo que sigue, suponemos que todos los anillos son conmutativos, con unidad, $1 \neq 0$, y de característica prima $p > 0$.

Sea $A \subseteq C$ una extensión de anillos con estas condiciones. Decimos que un elemento $x \in C$ tiene *exponente finito* si existe un entero $e \geq 0$ tal que $x^{p^e} \in A$, el menor entero con esta propiedad se conoce como el exponente del elemento. Decimos que la extensión de anillos $A \subseteq C$ tiene *exponente finito* si existe un entero $e \geq 0$ tal que todo elemento $x \in C$ tiene exponente como mucho e, o dicho de otro modo, tal que $x^{p^e} \in A$ para todo $x \in C$. El mínimo entero e que satisface esta propiedad se llama *exponente* de la extensión y lo denotamos por $\exp(C/A)$.

Las extensiones de cuerpos puramente inseparables son extensiones de cuerpos $K \subseteq L$ tales que cada elemento $x \in L$ tiene exponente finito sobre K. Han sido estudiadas ampliamente por autores como S. Shatz ([60]), S. U. Chase ([16]) y G. Pickert ([51], [52]). Nos centraremos en las extensiones finitas. En este caso, si $K \subseteq L$ es un extensión de cuerpos finita y puramente inseparable, se sabe que para cualquier clausura algebraica $\overline{K}$ del cuerpo K, tenemos un isomorfismo de $\overline{K}$-álgebras $L \otimes_K \overline{K} = \overline{K}[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$ para ciertos $e_i > 0$ (ver [54]). De hecho, las extensiones finitas puramente inseparables de cuerpos se pueden caracterizar entre las extensiones finitas usando esta propiedad que acabamos de describir.

Una versión similar de la propiedad anterior fue usada por F. Pauer en [49] para generalizar la noción de extensiones puramente inseparables al caso de anillos. En este contexto, el papel de la clausura algebraica es reemplazado por una extensión de

anillos fielmente plana. De manera más precisa, definiremos una extensión puramente inseparable de anillos como sigue:

Definición 0.1. Una extensión de anillos $A \subseteq C$ es *puramente inseparable* si cumple las siguientes condiciones:

(i) $A \subseteq C$ tiene exponente finito,

(ii) C es un A-módulo finitamente generado y proyectivo, y

(iii) para cada ideal primo $\mathfrak{p} \subset A$, hay una extensión fielmente plana $A_{\mathfrak{p}} \to A'$ de anillos tal que hay un isomorfismo $C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A' = A'[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$ para ciertos enteros $e_i > 0$.

El término original empleado por F. Pauer para nombrar a estas extensiones era *álgebras especiales*. Fue tiempo después cuando el término *puramente inseparable* se usó para referirse a estas extensiones ([55]). Advertimos al lector, que este término ha sido utilizado también en la literatura con otros matices. Por un lado, M. E. Sweedler lo usó también ([61]) con este mismo propósito de extender la definición de extensiones de cuerpos puramente inseparables a las álgebras sobre un anillo, pero con una perspectiva diferente. Más adelante, su definición de inseparabilidad fue considerada por A. Holleman, quien estableció una relación entre estas y las extensiones radiciales ([33]), y por S. Satô, quien la reformuló más adelante a una noción más fuerte ([57]). Estas otras definiciones de álgebras puramente inseparables son más amplias que la ofrecida por F. Pauer. De hecho, estas la incluyen como la subclase más pequeña que contiene a las extensiones de cuerpos puramente inseparables y que es cerrada por cambio de base y por descenso fielmente plano.

Por este motivo, nos acercaremos a las extensiones puramente inseparables de anillos desde la mencionada perspectiva de F. Pauer, que coincide con la dada por S. Yuan para el caso de exponente uno. Daremos más detalles más adelante, pero anticipamos algunas pistas. Por un lado, S. Yuan estudió las extensiones puramente inseparables de exponente uno, o *extensiones Galois* como las llamó, en relación con las p-bases ([68]) y también en términos del concepto de anillos diferencialmente simples ([66]). Por otro lado, F. Pauer dio en [49] una colección de condiciones equivalentes que caracterizaban las extensiones de anillos puramente inseparables en términos de los módulos de diferenciales y de las sucesiones normales de generadores, una noción que generaliza en cierto sentido el concepto de p-bases al caso de exponente mayor. Extendió algunas ideas de R. Rasala ([54]), que había tratado previamente el caso particular de las álgebras especiales sobre un cuerpo. Por nuestra parte, la principal contribución es extender la lista de caracterizaciones de las extensiones de anillos puramente inseparables usando operadores diferenciales.

Volviendo al caso de cuerpos, uno de los principales intereses relacionados con las extensiones puramente inseparables es desarrollar un teoría de "Galois" como la teoría clásica que se aplica a extensiones separables. A grandes rasgos, lo que se intenta es establecer una correspondencia entre ciertas subextensiones de una extensión de cuerpos puramente inseparable y ciertos subobjetos de un objeto algebraico. Encontramos diferentes aproximaciones a este problema, pero distinguimos dos de ellas.

El primer enfoque se centra en los subcuerpos intermedios de una extensión finita puramente inseparable de cuerpos. Es bien conocido que dada una extensión de cuerpos puramente inseparable $K \subseteq L$, cualquier subcuerpo intermedio E, i.e., $K \subseteq E \subseteq L$, es tal que las subextensiones $K \subseteq E$ y $E \subseteq L$ son también puramente inseparables. El caso de exponente uno fue tratado por N. Jacobson ([34], [36]), quien estableció una correspondencia biyectiva entre los cuerpos intermedios de una extensión finita puramente inseparable de cuerpos de exponente uno $K \subseteq L$ y las subálgebras de Lie restringidas de $\mathrm{Der}_K(L)$. Mientras que el caso general ha sido estudiado recientemente por L. Brantner and J. Waldron ([10]). Ellos extienden la correspondencia de Jacobson a todos los subcuerpos intermedios de cualquier extensión finita puramente inseparable de cuerpos $K \subseteq L$ usando pariticiones de algebroides de Lie y métodos de geometría algebraica derivada. Sin embargo, estamos lejos de obtener tal correspondencia para extensiones de anillos puramente inseparables. Como explicaremos más adelante, la situación en el caso de anillos conmutativos es más complicada, puesto que no todo subanillo intermedio B de una extensión de anillos puramente inseparable $A \subseteq C$ es tal que ambas extensiones $A \subseteq B$ y $B \subseteq C$ son puramente inseparables. De hecho, nuestra contribución en este sentido es aportar algunas condiciones que garantizan esta situación.

El segundo enfoque de las teorías "Galois" puramente inseparables se centra en algunos subcuerpos intermedios de una extensión finita puramente inseparable que juegan el papel de las extensiones normales en la teoría separable. Estos subcuerpos intermedios de interés son aquellos que inducen las subextensiones conocidas como *extensiones modulares*. Uno puede encontrar en [62], [23] y [15] algunas correspondencias, relacionadas con derivaciones de Hasse-Schmidt, para los subcuerpos intermedios E de una extensión de cuerpos finita puramente inseparable $K \subseteq L$ tal que $E \subset L$ es una extensión modular. La noción de extensión modular fue introducida por M. E. Sweedler en [62], que las caracterizó como extensiones finitas de cuerpos puramente inseparables $K \subseteq L$ que satisfacen las siguientes condiciones equivalentes:

(1) Hay un isomorfismo $L \simeq K[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}} - a_1, \ldots, X_n^{p^{e_n}} - a_n \rangle$ para algunos $a_i \in K$ y enteros $e_i > 0$.

(2) K es el cuerpo de constantes de el conjunto de derivaciones de orden superior de la extensión $K \subseteq L$.

(3) L^{p^e} y K son linealmente disjuntos para todo $e \geq 0$.

Recientemente, M. Wechter ha establecido en [64] otra caracterización de las extensiones de cuerpos modulares involucrando operadores diferenciales. Ha demostrado que la siguiente condición es equivalente a las anteriores para cualquier extensión finita puramente inseparable de cuerpos $K \subseteq L$:

(4) Para todo entero $e > 0$, el L-espacio vectorial $\mathrm{Diff}_K^{p^e}(L)$ está generado por el L^{p^e}-subespacio de operadores diferenciales $D \in \mathrm{Diff}_K^{p^e}(L)$ tales que $D(L^{p^k}) \subseteq L^{p^k}$ para todo $k \leq e$.

Como explicaremos más adelante, nuestra contribución en este tema es extender la definición de extensiones modulares al contexto de anillos usando una noción más

general de p-base, relacionada con la presentación dada en (1), y con la disjunción lineal como en (3).

Finalmente, observamos que hay también una correspondencia más general que aplica a cualquier extensión finita de cuerpos, no necesariamente de característica prima. Se conoce como la correspondencia de Jacobson-Bourbaki, que establece una correspondencia biyectiva entre los cuerpos intermedios de una extensión finita de cuerpos $K \subseteq L$ y las K-subálgebras unitarias del álgebra de endomorfismos lineales $\mathrm{End}_K(L)$ que son también L-subespacios vectoriales a izquierda ([38, I, §2, Theorem 2]). Esta correspondencia se ha extendido al caso no conmutativo de los anillos de división ([37], [31], [20]). Puesto que nuestro interés es generalizar algunos resultados que aplican para extensiones de cuerpos, es natural preguntarse si la correspondencia de Jacobson-Bourbaki se puede extender al caso de extensiones de anillos conmutativos. En este sentido, nuestra contribución es generalizar este teorema para extensiones de anillos conmutativos que son proyectivas y cuyos espectros son homeomorfos. En particular, esta correspondencia se puede aplicar a extensiones de anillos puramente inseparables.

Resultados principales y conclusiones

Los resultados incluidos en esta tesis provienen de dos fuentes. La primera es el artículo *Differentiably simple rings and ring extensions defined by p-basis* ([12]) publicado en *Journal of Pure and Applied Algebra* y escrito por la autora de la tesis en colaboración con D. Sulca y O. Villamayor. La segunda es una pre-publicación *Purely inseparable extensions of rings* ([11]), que es trabajo conjunto con D. Sulca. A continuación, damos una descripción de los resultados más relevantes obtenidos.

Extensiones puramente inseparables de exponente uno

Las extensiones de anillos puramente inseparables de exponente uno fueron introducidas por S. Yuan ([68]) bajo el nombre de *extensiones de Galois puramente inseparables de exponente uno*, o simplemente *extensiones Galois*. Las definió como sigue:

Definición 0.2. Una extensión finita de anillos $A \subseteq C$ es una *extensión Galois de exponente uno* si:

(i) $A \subseteq C$ tiene exponente como mucho uno, i.e., $C^p \subseteq A$,

(ii) C es un A-módulo proyectivo, y

(iii) para cada ideal primo $\mathfrak{p} \subset A$, la extensión $A_\mathfrak{p} \subseteq C_\mathfrak{p} := C \otimes_A A_\mathfrak{p}$ admite una p-base, i.e., existe un isomorfismo $C_\mathfrak{p} \simeq A_\mathfrak{p}[X_1, \ldots, X_n]/\langle X_1^p - a_1, \ldots, X_n^p - a_n\rangle$ de $A_\mathfrak{p}$-álgebras para ciertos $a_i \in A_\mathfrak{p}$.

S. Yuan estudió la relación entre estas extensiones y los anillos diferencialmente simples ([66]) y las derivaciones ([68]). De hecho, sus resultados muestran que la condición (iii) en la definición anterior pueden reemplazarse por cualquiera de las siguientes propiedades:

(v) para cada ideal primo $\mathfrak{p} \subset A$, el anillo $C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ es diferencialmente simple, i.e., los únicos ideales $I \subseteq C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ tales que $D(I) \subseteq I$ para toda derivación D son el ideal trivial y el propio anillo.

(vi) $\mathrm{End}_A(C) = C[\mathrm{Der}_A(C)]$ como A-álgebras.

Además, E. Kunz exploró la conexión entre las p-bases y los módulos de diferenciales de Kähler ([44]). Usando su perspectiva, las extensiones Galois de exponente uno se pueden caracterizar como extensiones de anillos $A \subseteq C$ de exponente uno tales que el módulo de diferenciales $\Omega_{C/A}$ es un C-módulo proyectivo.

En esta tesis, estudiamos las extensiones puramente inseparables de exponente uno desde la perspectiva de los operadores diferenciales. En la Sección 2.2 del segundo capítulo, probamos la Proposición 2.62 y la Proposición 2.67, que llevan a la siguiente nueva caracterización de las extensiones Galois:

Teorema 0.3. *Sea $A \subseteq C$ una extensión finita de anillos de exponente como mucho uno. Entonces $A \subseteq C$ es puramente inseparable si y solo si C es un A-módulo proyectivo y $\mathrm{Der}_A(C)$ es un C-sumando directo de $\mathrm{End}_A(C)$.*

También revisamos y ofrecemos nuevas pruebas para las caracterizaciones resultantes del trabajo de S. Yuan y E. Kunz. Resumimos estas caracterizaciones en el siguiente teorema, que puede encontrarse en la Sección 2.2.

Teorema 0.4. *Dada una extensión finita de anillos de exponente como mucho uno $A \subseteq C$, son equivalentes:*

(1) $A \subseteq C$ es una extensión puramente inseparable (como en la Definición 0.1).

(2) $A \subseteq C$ es una extensión Galois (como en la Definición 0.2).

(3) C es un A-módulo proyectivo, y $C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ es diferencialmente simple para cada ideal primo $\mathfrak{p} \subset A$.

(4) $\Omega_{C/A}$ es un C-módulo proyectivo.

(5) C es un A-módulo proyectivo y $\mathrm{End}_A(C) = C[\mathrm{Der}_A(C)]$.

(6) C es un A-módulo proyectivo y $\mathrm{Der}_A(C)$ es un C-sumando directo de $\mathrm{End}_A(C)$.

Uno de nuestros objetivos es generalizar este teorema al contexto de extensiones de anillos de exponente mayor, es decir, obtener caracterizaciones para extensiones de anillos puramente inseparables de exponente finito cualquiera.

Volviendo a la perspectiva original de S. Yuan, su motivación radicaba en desarrollar una teoría de Galois para las extensiones de anillos puramente inseparables de exponente uno. Consiguió extender la correspondencia de Jacobson para extensiones de cuerpos ([36]) al contexto de extensiones Galois de exponente uno. Concretamente, probó que cada subanillo intermedio B de una extensión de Galois $A \subseteq C$, tal que $B \subseteq C$ es también Galois, se corresponde unívocamente con una subálgebra de Lie

restringida de $\mathrm{Der}_A(C)$ que es a su vez un C-sumando directo de $\mathrm{Der}_A(C)$ como C-módulo ([68, Theorem 13]). También demostró que tal subanillo intermedio B cumple que $A \subseteq B$ es Galois ([68, Theorem 11]). Después, usando métodos homológicos, M. André caracterizó estos subanillos intermedios como aquellos tales que C es proyectivo como B-módulo ([1, Théorème 71]).

En esta tesis, nos centramos en las torres Galois de anillos de rango diferencial fijo, es decir, torres de anillos $A \subseteq B \subseteq C$ tales que $A \subseteq C$, $B \subseteq C$ y $A \subseteq B$ son extensiones Galois de exponente uno tales que los C-módulos $\Omega_{C/A}$ y $\Omega_{C/B}$ tienen rango constante. Dada una extensión Galois $A \subseteq C$, tal que $\Omega_{C/A}$ tiene rango constante como C-módulo, definimos un functor cuyo conjunto de A-puntos es el conjunto de torres Galois de rango diferencial fijo.

Definición 0.5. Dada una extensión Galois $A \subseteq C$, tal que $\Omega_{C/A}$ tiene rango constante n como C-módulo, y dado un entero fijo $0 \leq r \leq n$, el *functor de Yuan* asociado a $A \subseteq C$ y r es el functor covariante de la categoría de A-álgebras en la categoría de conjuntos dado por

$$\begin{aligned} \mathcal{Y}^r_{C/A}\colon \mathrm{Alg}_A &\to \mathrm{Sets} \\ A' &\mapsto \left\{ B' \text{ subanillo} : \begin{array}{l} A' \subseteq B' \subseteq C \otimes_A A' =: C', \\ B' \subseteq C' \text{ es Galois y } \Omega_{C'/B'} \text{ tiene rango } r \end{array} \right\}. \end{aligned}$$

En la Sección 2.3 del segundo capítulo, probamos que este functor es representable por un esquema sobre A quasi-proyectivo (Teorema 2.92) y estudiamos algunas de las propiedades geométricas (Teorema 2.95). Más precisamente, probamos el siguiente resultado:

Teorema 0.6. *Dada una extensión Galois $A \subseteq C$, tal que $\Omega_{C/A}$ tiene rango constante n como C-módulo, y un entero fijo $0 \leq r \leq n$, el functor de Yuan $\mathcal{Y}^r_{C/A}$ es representable por un esquema sobre A quasi-proyectivo y liso que tiene fibras lisas irreducibles de dimensión $(p^n - p^{n-r})(n-r)$.*

Extensiones puramente inseparables de exponente mayor

Regresamos al caso de exponente mayor. Como hemos mencionado, las extensiones de anillos puramente inseparables fueron introducidas como *álgebras especiales* por F. Pauer ([49]). Las presentó como extensiones finitas de anillos $A \subseteq C$ de exponente finito que satisfacen las siguientes condiciones equivalentes:

(1) C es un A-módulo proyectivo, y para cada ideal primo $\mathfrak{p} \subset A$, existe una extensión de anillos fielmente plana $A_\mathfrak{p} \to A'$ que induce un isomorfismo de A'-álgebras $C_\mathfrak{p} \otimes_{A_\mathfrak{p}} A' = A'[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$ para algunos $e_i > 0$.

(2) C es un A-módulo proyectivo y para cada ideal primo $\mathfrak{p} \subset A$, hay enteros positivos $e_1 \geq \cdots \geq e_n$ y polinomios $P_i \in A_\mathfrak{p}[X_1, \ldots, X_{i-1}]$ para $i = 1, \ldots, n$, tales que $C_\mathfrak{p}$ admite una presentación como $A_\mathfrak{p}$-álgebra $C_\mathfrak{p} = A_\mathfrak{p}[x_1, \ldots, x_n]$ definida por las relaciones $x_i^{p^{e_i}} = P_i(x_1^{p^{e_i}}, \ldots, x_{i-1}^{p^{e_i}})$ para $i = 1, \ldots, n$.

(3) El módulo de diferenciales $\Omega_{A[C^{p^e}]/A}$ es un $A[C^{p^e}]$-módulo proyectivo para todo $e \geq 0$.

En cierto sentido, estas equivalencias pueden verse como una generalización al caso de exponente mayor de las equivalencias (1)⇔(2)⇔(4) del Teorema 0.4 que resume las caracterizaciones de las extensiones puramente inseparables de exponente uno.

Más tarde, P. Sancho de Salas estudió la noción de *álgebra diferencialmente homogénea*, es decir, una A-álgebra C que es plana, de presentación finita y tal que el módulo de partes principales $\mathrm{P}^k_{C/A}$ es proyectivo sobre C para todo $k \geq 0$. Probó en [56] que las extensiones puramente inseparables son álgebras diferencialmente homogéneas de exponente finito. En otras palabras, demostró que para una extensión finita de anillos $A \subseteq C$ de exponente finito la siguiente condición es equivalente a las tres propiedades enunciadas previamente:

(4) El módulo de partes principales $\mathrm{P}^k_{C/A}$ es proyectivo sobre C para todo $k \geq 0$.

En esta tesis, alargamos la lista de equivalencias usando operadores diferenciales. En la Sección 3.2 del tercer capítulo, probamos un resultado de extensión de operadores diferenciales (Proposición 3.39), que nos permite enunciar una nueva caracterización de las extensiones puramente inseparables en términos de ciertos módulos de operadores diferenciales. Como una combinación de la Proposición 3.47 y la Proposición 3.43, obtenemos una caracterización de las extensiones puramente inseparables que generaliza el Teorema 0.3 al caso de exponente mayor del siguiente modo:

Teorema 0.7. *Sea $A \subseteq C$ una extensión finita de anillos de exponente finito. Entonces $A \subseteq C$ es puramente inseparable si y solo si C es un $A[C^{p^e}]$-módulo proyectivo para todo $e \geq 0$, y el módulo de operadores diferenciales $\mathrm{Diff}^{p^e}_A(C)$ es un C-sumando directo de $\mathrm{End}_A(C)$ como C-módulo para todo $e \geq 0$.*

Además, usando técnicas de operadores diferenciales, volvemos a obtener desde una perspectiva distinta la caracterización en términos de los módulos de partes principales correspondiente a la propiedad (4) anterior. En conclusión, podemos resumir las caracterizaciones para extensiones de anillos puramente inseparables en el siguiente teorema:

Teorema 0.8. *Dada una extensión finita de anillos $A \subseteq C$ de exponente finito, son equivalentes:*

(1) $A \subseteq C$ es puramente inseparable (como en la Definición 0.1).

(2) C es un A-módulo proyectivo y para cada ideal primo $\mathfrak{p} \subset A$, la extensión de anillos $A_\mathfrak{p} \subseteq C_\mathfrak{p}$ es una sucesión normal de generadores, i.e., existe una presentación $C_\mathfrak{p} = A_\mathfrak{p}[x_1, \ldots, x_n]$ definida por las relaciones $x_i^{p^{e_i}} = P_i(x_1^{p^{e_i}}, \ldots, x_{i-1}^{p^{e_i}})$ para ciertos enteros $e_1 \geq \cdots \geq e_n > 0$ y polinomios $P_i \in A_\mathfrak{p}[X_1, \ldots, X_{i-1}]$, para $i = 1, \ldots, n$.

(3) El módulo de diferenciales $\Omega_{A[C^{p^e}]/A}$ es un $A[C^{p^e}]$-módulo proyectivo para todo entero $e \geq 0$.

(4) C es un $A[C^{p^e}]$-módulo proyectivo y el C-módulo de operadores diferenciales $\mathrm{Diff}_A^{p^e}(C)$ es un sumando directo de $\mathrm{End}_A(C)$ como C-módulo, para todo $e \geq 0$.

(5) El módulo de partes principales $\mathrm{P}_{C/A}^{p^e}$ es proyectivo sobre C para todo $e \geq 0$.

Torres puramente inseparables de anillos

Continuamos con las torres puramente inseparables. Como hemos explicado anteriormente, uno de los principales intereses de la teoría puramente inseparable de cuerpos es comprender las subextensiones intermedias de una extensión puramente inseparable y establecer alguna correspondencia entre estas y otros subobjetos de otro objeto algebraico. Estamos interesados en la comprensión de las *torres puramente inseparables* de anillos, es decir, torres de anillos $A \subseteq B \subseteq C$ tales que $A \subseteq C$, $B \subseteq C$ y $A \subseteq B$ son extensiones puramente inseparables.

En el caso de exponente uno, dada una extensión Galois $A \subseteq C$, M. André probó que los subanillos intermedios B que inducen torres puramente inseparables son exactamente aquellos tales que C es proyectivo como B-módulo. Sin embargo, la situación se complica cuando tratamos con exponente mayor. Si $A \subseteq C$ es una extensión puramente de exponente mayor que uno y B es un subanillo intermedio tal que C es proyectivo como B-módulo, no es cierto en general que $A \subseteq B$ y $B \subseteq C$ sean también puramente inseparables (ver Ejemplo 3.52). Por tanto, en esta tesis, mostraremos algunas condiciones para los subanillos intermedios B de una extensión puramente inseparable $A \subseteq C$ que garantizan que ambas subextensiones $A \subseteq B$ y $B \subset C$ son también puramente inseparables. Con este propósito, introducimos la siguiente clase de extensiones de anillos:

Definición 0.9. Una extensión finita de anillos $A \subseteq C$ de exponente finito es una *$\mathcal{F}$-extensión* si C es un $A[C^{p^e}]$-módulo proyectivo para todo $e \geq 0$.

Observamos que toda extensión puramente inseparable es en particular una $\mathcal{F}$-extensión. En la Sección 3.3, probamos que imponiendo esta condición a ciertas subextensiones de una extensión puramente inseparable $A \subseteq C$ relacionadas con el subanillo intermedio B, obtenemos una torre puramente inseparable $A \subseteq B \subseteq C$. De manera más precisa, demostramos:

Teorema 0.10. *Sea $A \subseteq C$ una extensión de anillos puramente inseparable y sea B un subanillo intermedio tal que $A \subseteq B$ y $B \subseteq C$ son $\mathcal{F}$-extensiones. Si $A \subseteq B[C^{p^e}]$ es una $\mathcal{F}$-extensión para todo $e \geq 1$, entonces $A \subseteq B \subseteq C$ es una torre puramente inseparable.*

Usando el teorema anterior, obtenemos la siguiente caracterización para las torres puramente inseparables de exponente dos:

Corolario 0.11. *Sea $A \subset C$ una extensión de anillos puramente inseparable de exponente dos y sea B un subanillo intermedio. Entonces $A \subseteq B \subseteq C$ es una torre puramente inseparable si y solo si $A \subseteq B$ y $B \subseteq C$ son ambas $\mathcal{F}$-extensiones.*

Además, estudiamos cuándo la composición de dos extensiones puramente inseparables $A \subseteq B$ y $B \subseteq C$ inducen una torre puramente inseparable $A \subseteq B \subseteq C$. Mostramos que esto ocurre si imponemos algunas condiciones adicionales:

Teorema 0.12. *Sean $A \subseteq B$ y $B \subseteq C$ extensiones de anillos puramente inseparables. Si $A \subset B[C^{p^e}]$ es una $\mathcal{F}$-extensión para todo $e \geq 0$, entonces $A \subset C$ es también puramente inseparable.*

Por último señalamos que, como no comprendemos completamente las torres de extensiones puramente inseparables, estamos lejos de obtener una teoría de Galois puramente inseparable para anillos como las que han sido desarrolladas en el caso de cuerpos. No obstante, al trabajar con estas extensiones, hemos obtenido una generalización de la correspondencia de Jacobson-Bourbaki para subcuerpos intermedios de una extensión finita de cuerpos cualquiera ([38, I, §2, Theorem 2]) al caso de ciertas subextensiones de anillos conmutativos de cualquier característica. De hecho, demostramos en la Sección 1.3 del primer capítulo el siguiente resultado, que es aplicable para extensiones de anillos puramente inseparables.

Theorem 0.1. *Sea $A \subseteq C$ una extensión finita de anillos tal que C es proyectivo como A-módulo. Supongamos que el morfismo inducido* $\mathrm{Spec}(C) \to \mathrm{Spec}(A)$ *es un homeomorfismo. Entonces hay una biyección entre el subconjunto de anillos*

$$\mathcal{P}_{C/A} := \left\{ B : \begin{array}{l} B \text{ es un subanillo intermedio } A \subseteq B \subseteq C \\ \text{y } C \text{ es un } B\text{-módulo proyectivo} \end{array} \right\} \Bigg($$

y el subconjunto de subálgebras

$$\mathcal{D}_{C/A} := \left\{ H : \begin{array}{l} H \text{ es una } A\text{-subálgebra unitaria de } \mathrm{End}_A(C) \text{ y} \\ \text{un sumando directo de } \mathrm{End}_A(C) \text{ como } C\text{-módulo} \end{array} \right\} \Bigg($$

dado por las siguientes aplicaciones inversas

$$\begin{array}{cccc} \mathcal{P}_{C/A} & \to \mathcal{D}_{C/A}, & \mathcal{D}_{C/A} & \to \mathcal{P}_{C/A} \\ B & \mapsto \mathrm{End}_B(C) & H & \mapsto B_H := \{x \in C : [\varphi, x] = 0,\ \forall \varphi \in H\}. \end{array}$$

Extensiones modulares de anillos

Hemos mencionado que hay una subclase de extensiones de cuerpos puramente inseparables que es particularmente interesante, esto es, las extensiones modulares. En esta tesis, extendemos la noción original de extensiones modulares de cuerpos al contexto de anillos. Siguiendo una de las caracterizaciones de M. E. Sweedler ([62, Theorem 1]) y usando la noción de p-bases generalizadas introducida por S. Yuan ([67]), definimos las extensiones modulares de anillos como sigue:

Definition 0.2. Una extensión finita de anillos $A \subseteq C$ es una *extensión modular* si

(1) $A \subseteq C$ tiene exponente finito, i.e., $C^{p^e} \subseteq A$ para algún $e \geq 0$;

(2) C es un A-módulo proyectivo; y

(3) para cada ideal primo $\mathfrak{p} \subset A$, la extensión $A_\mathfrak{p} \subseteq C_\mathfrak{p}$ tiene una p-base generalizada, i.e., hay un isomorfismo $C_\mathfrak{p} \simeq A_\mathfrak{p}[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}} - a_1, \ldots, X_n^{p^{e_n}} - a_n\rangle$ de $A_\mathfrak{p}$-álgebras para algunos $a_i \in A_\mathfrak{p}$ y enteros $e_i > 0$.

En la Sección 4.2 del cuarto capítulo, mostramos que cualquier extensión modular de anillos es puramente inseparable (Proposición 4.33). También las caracterizamos entre las extensiones puramente inseparables como aquellas que satisfacen una condición de disjunción lineal (Teorema 4.38), como ocurre en el caso de cuerpos. Más precisamente, nuestro resultado final es:

Teorema 0.13. *Sea $A \subseteq C$ una extensión finita de anillos de exponente finito. Entonces $A \subseteq C$ es modular si y solo si $A \subseteq C$ es puramente inseparable, y los anillos C^{p^e} y A son linealmente disjuntos para todo $e \geq 0$.*

Algunas preguntas abiertas

Se puede percibir que el tema de las extensiones puramente inseparables de anillos no está agotado y que quedan algunas preguntas naturales por responder. Incluimos a continuación algunas de estas preguntas que en las que esperamos trabajar en el futuro.

Anillos diferencialmente simples y extensiones de exponente superior. Recordamos que un anillo R es diferencialmente simple si los únicos ideales $I \subseteq R$ tales que $D(I) \subseteq I$ para cualquier derivación $D\colon R \to R$ son 0 y R. Como repasamos en la Subsección 2.1.4 del segundo capítulo, L. R. Harper demostró que cualquier anillo Noetheriano diferencialmente simple A de característica p tiene una presentación $A \simeq K[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p\rangle$ para cierto cuerpo de coeficientes K. Usando esta noción de anillo diferencialmente simple, las extensiones puramente inseparables de exponente uno se pueden caracterizar como extensiones finitas de anillos $A \subseteq C$ de exponente uno tales que C es un A-módulo proyectivo y $C_\mathfrak{p}/\mathfrak{p}C_\mathfrak{p}$ es diferencialmente simple para cada ideal primo $\mathfrak{p} \subset A$. Continuando con el trabajo de S. Yuan en [67], es natural preguntarse si esta caracterización se puede extender al caso de exponente mayor, es decir, si se puede definir una noción similar de anillos diferencialmente simples usando derivaciones de Hasse-Schmidt u operadores diferenciales de orden superior, que nos permita caracterizar las extensiones puramente inseparables de exponente mayor y tal que exista un análogo del teorema de estructura de Harper.

Una correspondencia de Galois para torres puramente inseparables de anillos. En el caso de exponente uno, sabemos que los subanillos intermedios B de una extensión Galois de exponente uno $A \subseteq C$, tal que $A \subseteq B$ y $B \subseteq C$ son también Galois, son aquellos tales que C es un B-módulo proyectivo. También sabemos que estos subanillos intermedios están en correspondencia biyectiva con ciertas subálgebras de Lie de $\mathrm{Der}_A(C)$. Para el caso de exponente mayor, hemos encontrado condiciones suficientes para que un subanillo intermedio B de una extensión puramente inseparable de anillos $A \subseteq C$ induzca una torre puramente inseparable $A \subseteq B \subseteq C$. Nos gustaría encontrar las condiciones necesarias sobre estos subanillos intermedios para que esta situación ocurra. En otras palabras, queremos caracterizar todos los subanillos intermedios B de una extensión puramente inseparable de anillos $A \subseteq C$ tal que $A \subseteq B \subseteq C$ es una torre

puramente inseparable. Además, si uno pudiera obtener tal caracterización, también querría trabajar en otras dos direcciones. Por un lado, establecer una correspondencia entre estos subanillos y otros subobjetos de un objeto algebraico, generalizando la ya conocida correspondencia de Yuan para exponente uno. Por otro lado, definir un functor representable, como el functor de Yuan para el caso de exponente uno (ver Definición 0.5), que parametriza estas subextensiones intermedias.

Extensiones modulares y operadores diferenciales. Está claro que los operadores diferenciales juegan un papel importante en el estudio de las extensiones puramente inseparables. Los recientes resultados de M. Wechter [64] muestran que hay también una conexión con las extensiones modulares de cuerpos. Nos gustaría entender esta relación y, si es posible, generalizarla al contexto de anillos. Esto es, nos gustaría obtener una caracterización de las extensiones modulares usando operadores diferenciales.

Resumen de contenidos

La tesis está organizada en cuatro capítulos, que contienen todos los resultados explicados anteriormente, y un breve apéndice, que recopila algunos resultados básicos del Álgebra Conmutativa que se usan sistemáticamente a lo largo de la tesis.

El Capítulo 1 está dedicado a los módulos proyectivos. Ofrecemos una breve introducción a estas estructuras algebraicas, en particular, a las extensiones finitas de anillos $A \subseteq C$ tales que C es proyectivo como A-módulo. Repasamos algunas propiedades básicas que serán utilizadas frecuentemente en la tesis. También nos centramos en algunas subextensiones intermedias de extensiones finitas y proyectivas de anillos. En este contexto, demostramos una generalización del la correspondencia de Jacobson-Bourbaki establecida el Teorema 0.1.

El Capítulo 2 estudia las extensiones de anillos puramente inseparables de exponente uno, o extensiones Galois (ver Definición 0.2). Incluimos aquí algunos preliminares sobre derivaciones, diferenciales de Kähler, p-bases y anillos diferencialmente simples, que son conceptos que se usan para caracterizar las extensiones Galois. Considerando las derivaciones como operadores diferenciales de orden uno, probamos el Teorema 0.3 que nos da una caracterización para estas extensiones. Además, repasamos el concepto de torres Galois de anillos y definimos el functor de Yuan como en la Definición 0.5. Demostramos el Teorema 0.6 sobre representabilidad del functor de Yuan por un esquema y estudiamos sus propiedades geométricas.

El Capítulo 3 se ocupa de las extensiones de anillos puramente inseparables en general (Definición 0.1). Primero revisamos las caracterizaciones originales de F. Pauer en términos de sucesiones normales de generadores y los módulos de diferenciales. Después estudiamos estas extensiones desde la perspectiva de los operadores diferenciales y obtenemos una caracterización en el Teorema 0.7. También usamos estas técnicas de operadores diferenciales para volver a obtener una caracterización que involucra a los módulos de partes principales. En conclusión, obtenemos el Teorema 0.8. Además, estudiamos las torres puramente inseparables de anillos y ofrecemos condiciones suficientes para que una torre de anillos $A \subseteq B \subseteq C$ sea puramente inseparable. Estas condiciones se condensan en Teorema 0.10, Corolario 0.11 y Teorema 0.12.

El Capítulo 4 se enfoca en la extensiones modulares de anillos Comenzamos con algunos preliminares sobre disjunción lineal y p-bases generalizadas. Después, los usamos para extender la definición original de extensiones modulares de cuerpos al caso de anillos (Definición 0.2). Probamos que estas extensiones son exactamente las extensiones puramente inseparables que satisfacen ciertas propiedades de disjunción lineal como en el Teorema 0.13.

Para facilitar la lectura, cada capítulo incluye al inicio una breve introducción y una visión general de la organización de las secciones.

Introduction

Purely inseparable extensions of fields are an object of interest in Commutative Algebra. They have been studied extensively, in particular with a view to develop an analogue of the classical Galois theory established for separable field extensions. The main objective of this thesis is to study the extension of the notion of purely inseparable extensions to the setting of rings and to generalize some of the properties and results that are already known for purely inseparable field extensions to this broader context.

Keywords: Purely inseparable extensions of rings, towers of rings, differential operators, p-basis, projective modules, modular extensions

MSC Classification Codes: 13B05, 13N10, 13C10, 14M15, 14L17

Motivation

For now on, we consider all the rings to be commutative with unity, $1 \neq 0$, and of prime characteristic $p > 0$.

Let $A \subseteq C$ be such a ring extension. An element $x \in C$ is said to have *finite exponent* if there exists an integer $e \geq 0$ such that $x^{p^e} \in A$, and the minimal integer with this property is known as the exponent of the element. The ring extension $A \subseteq C$ is said to have *finite exponent* if there is an integer $e \geq 0$ such that every element $x \in C$ has exponent at most e, or, such that $x^{p^e} \in A$ for any $x \in C$. The minimal e satisfying this condition is called the *exponent* of the extension and we denote it by $\exp(C/A)$.

Purely inseparable extensions of fields are field extensions $K \subseteq L$ such that every element $x \in L$ has finite exponent over K. They have been widely studied by authors as S. Shatz ([60]), S. U. Chase ([16]) and G. Pickert ([51], [52]). We will focus on finite extensions. In this case, if $K \subseteq L$ is a finite purely inseparable field extension, it is well-known that for any algebraic closure $\overline{K}$ of the field K, we have an isomorphism of $\overline{K}$-algebras $L \otimes_K \overline{K} = \overline{K}[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$ for some $e_i > 0$ (see [54]). In fact, finite purely inseparable field extensions can be characterized among finite field extensions by the described property.

A similar version of the above property was used by F. Pauer in [49] to generalize the notion of purely inseparable extension to the setting of rings. In this context, the role of the algebraic closure is replaced by a faithfully flat extension of rings. More precisely, we define a purely inseparable ring extension as follows:

Definition 0.3. A ring extension $A \subseteq C$ is *purely inseparable* if it satisfies the next conditions:

(i) $A \subseteq C$ has finite exponent,

(ii) C is a finitely generated projective A-module, and

(iii) for each prime ideal $\mathfrak{p} \subset A$, there is a faithfully flat ring extension $A_{\mathfrak{p}} \to A'$ such that there is an isomorphism $C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A' = A'[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$ for some $e_i > 0$.

The original term used by F. Pauer to name these extensions was that of *special algebras*. It was some time later when the term *purely inseparable* was used to refer to these extensions ([55]). We should warn the reader that this term has been also used in the literature with different meanings. In fact, M. E. Sweedler also used it ([61]) with the same purpose of extending the definition of purely inseparable extension of fields to algebras over a ring from a different perspective. Then his definition for inseparability was considered by A. Holleman, who stated a relation between these and radicial extensions ([33]), and by S. Satô, who reformulated it later into a stronger notion ([57]). These other definitions of purely inseparable algebras are wider than the one given by F. Pauer. In fact, they include it as the smaller subclass containing purely inseparable field extensions that is closed by base change and faithfully flat descent.

For this reason, we will approach purely inseparable ring extensions from the mentioned perspective given by F. Pauer, which coincides with the one given by S. Yuan for the exponent one case. We will go into more detail later, but we anticipate some hints. On the one hand, S. Yuan studied purely inseparable extensions of exponent one, or *Galois extensions* as he called them, in relation with p-basis ([68]) and also in terms of the notion of differentiably simple rings ([66]). On the other hand, F. Pauer gave in [49] a collection of equivalent conditions that characterize purely inseparable ring extensions in terms of the modules of differentials and the normal generating sequences, a notion that generalizes in some sense the concept of p-basis to the higher exponent setting. He extended some ideas from R. Rasala ([54]), who treated previously the particular case of special algebras over a field. By our side, our main contribution is to enlarge the list of characterizations of purely inseparable extensions of rings using differential operators.

Returning to the setting of fields, one of the principal interests related to purely inseparable field extensions is to develop a "Galois" theory as the classical one that holds for separable extensions. Roughly speaking, it is intended to establish a correspondence between certain subextensions of a purely inseparable field extension and certain subobjects of an algebraic object. There have been different approaches with this purpose, but we distinguish two of them.

The first approach focuses on the intermediate subfields of a finite purely inseparable field extension. It is well-known that given a purely inseparable field extension $K \subseteq L$, any intermediate subfield E, i.e., $K \subseteq E \subseteq L$, is such that the subextensions $K \subseteq E$ and $E \subseteq L$ are also purely inseparable. The exponent one case was treated

by N. Jacobson ([34], [36]), who established a one-to-one correspondence between the intermediate fields of a finite purely inseparable field extension of exponent one $K \subseteq L$ and restricted Lie subalgebras of $\mathrm{Der}_K(L)$. While the general case has been studied recently by L. Brantner and J. Waldron ([10]). They extend Jacobson's correspondence to all the intermediate subfields of an arbitrary finite purely inseparable field extension $K \subseteq L$ by using partition Lie algebroids and methods of derived algebraic geometry. However, we are far from obtaining such a correspondence for purely inseparable ring extensions. As we will explain later, the situation in the case of commutative rings is more complicated, since not every intermediate subring B of a purely inseparable ring extension $A \subseteq C$ is such that both $A \subseteq B$ and $B \subseteq C$ are purely inseparable. In fact, our contribution in this direction is to give some conditions that ensure that this situation occurs.

The second approach of purely inseparable "Galois" theories is to focus on some intermediate subfields of a finite purely inseparable extension that play the role of normal extensions in the separable theory. These intermediate subfields of interest are those that induce the subextensions known as *modular extensions*. One can find in [62], [23] and [15] some correspondences, related to the Hasse-Schmidt derivations, for the intermediate subfields E of a finite purely inseparable field extension $K \subseteq L$ such that $E \subset L$ is a modular extension. The notion of modular extension was introduced by M. E. Sweedler in [62], who characterized them as finite purely inseparable field extensions $K \subseteq L$ that satisfy the following equivalent conditions:

(1) There is an isomorphism $L \simeq K[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}} - a_1, \ldots, X_n^{p^{e_n}} - a_n \rangle$ for some $a_i \in K$ and $e_i > 0$.

(2) K is the field of constants of the set of higher derivations of the extension $K \subseteq L$.

(3) L^{p^e} and K are linearly disjoint for all $e \geq 0$.

Recently, another characterization of modular field extensions involving differential operators has been stated by M. Wechter ([64]). He has proved that the next condition is equivalent to previous ones for any finite purely inseparable field extension $K \subseteq L$:

(4) For any integer $e > 0$, the L-vector space $\mathrm{Diff}_K^{p^e}(L)$ is generated by the L^{p^e}-subspace of differential operators $D \in \mathrm{Diff}_K^{p^e}(L)$ such that $D(L^{p^k}) \subseteq L^{p^k}$ for all $k \leq e$.

As we will explain later, our contribution on this topic is to extend the definition of modular extensions to the setting of rings using a generalized notion of p-basis, related to the presentation given in (1), and linearly disjointedness as in (3).

Finally, we observe that there is also a more general correspondence that applies for any finite extension of fields, not necessarily of prime characteristic. It is known as the Jacobson-Bourbaki correspondence, which establishes a one-to-one correspondence between the intermediate fields of a finite field extension $K \subseteq L$ and the unital K-subalgebras of the algebra of linear endomorphisms $\mathrm{End}_K(L)$ that are also left L-vector subspaces ([38, I, §2, Theorem 2]). This correspondence has been extended to

the non-commutative setting of division rings ([37], [31], [20]). Since our interest is to generalize some results that apply to field extensions, it is natural to ask if the Jacobson-Bourbaki correspondence can be extended to the setting of commutative ring extensions. In this sense, our contribution is a generalization of this theorem for commutative ring extensions that are projective and have homeomorphic spectra, which applies in particular to purely inseparable ring extensions.

Main results and conclusions

The results included in these thesis can be found in two sources. The first one is the article *Differentiably simple rings and ring extensions defined by p-basis* ([12]) published in the *Journal of Pure and Applied Algebra* and written by the author of the thesis in collaboration with D. Sulca and O. Villamayor. The second one is the pre-print *Purely inseparable extensions of rings* ([11]), which is joint work with D. Sulca. We give now a description of the main results in the order in which they were obtained.

Purely inseparable extensions of exponent one

Purely inseparable rings extensions of exponent one were introduced by S. Yuan ([68]), under the name of *purely inseparable Galois extensions of exponent one*, or simply *Galois extensions*. He defined them as:

Definition 0.4. A finite extension of rings $A \subseteq C$ is a *Galois extension of exponent one* if:

(i) $A \subseteq C$ has exponent at most one, i.e., $C^p \subseteq A$,

(ii) C is a projective A-module, and

(iii) for each prime ideal $\mathfrak{p} \subset A$, the extension $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}} := C \otimes_A A_{\mathfrak{p}}$ admits a p-basis, i.e., there is an isomorphism $C_{\mathfrak{p}} \simeq A_{\mathfrak{p}}[X_1, \ldots, X_n]/\langle X_1^p - a_1, \ldots, X_n^p - a_n\rangle$ of $A_{\mathfrak{p}}$-algebras for some $a_i \in A_{\mathfrak{p}}$.

S. Yuan studied the relation of these extensions with differentiably simple rings ([66]) and derivations ([68]). In fact, his results show that condition (iii) in the above definition can be replaced by any of the following properties:

(v) for each prime ideal $\mathfrak{p} \subset A$, the ring $C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ is differentiably simple, i.e., the only ideals $I \subseteq C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ such that $D(I) \subseteq I$ for any derivation D are the trivial ideal and the ring itself.

(vi) $\mathrm{End}_A(C) = C[\mathrm{Der}_A(C)]$ as A-algebras.

Moreover, E. Kunz explored the connection between p-basis and the modules of Kähler differentials ([44]). So, using his perspective, Galois extensions of exponent one can be characterized as ring extensions $A \subseteq C$ of exponent one such that the module of differentials $\Omega_{C/A}$ is a projective C-module.

In this thesis, we study purely inseparable extensions of exponent one from the perspective of differential operators. In Section 2.2 in the second chapter, we prove Proposition 2.62 and Proposition 2.67, which lead to the following new characterization of Galois extensions:

Theorem 0.5. *Let $A \subseteq C$ be a finite ring extension of exponent at most one. Then $A \subseteq C$ is purely inseparable if and only if C is a projective A-module and $\mathrm{Der}_A(C)$ is a C-direct summand of $\mathrm{End}_A(C)$.*

We also revisit and give some new proofs for the characterizations resulting from the work of S. Yuan and E. Kunz. We summarize all the mentioned characterizations in the next theorem, which can be found at the end of Section 2.2.

Theorem 0.6. *For a finite ring extension of exponent at most one $A \subseteq C$, the following are equivalent:*

(1) $A \subseteq C$ is a purely inseparable extension (as in Definition 0.3).

(2) $A \subseteq C$ is a Galois extension (as in Definition 0.4).

(3) C is a projective A-module and $C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ is differentiably simple for each prime ideal $\mathfrak{p} \subset A$.

(4) $\Omega_{C/A}$ is a projective C-module.

(5) C is a projective A-module and $\mathrm{End}_A(C) = C[\mathrm{Der}_A(C)]$.

(6) C is a projective A-module and $\mathrm{Der}_A(C)$ is a C-direct summand of $\mathrm{End}_A(C)$.

One of our aims is to generalize this theorem to the setting of ring extensions of higher exponent, that is, to obtain characterizations for purely inseparable ring extensions of arbitrary exponent.

Returning to the original perspective of S. Yuan, his motivation was to develop a Galois theory for purely inseparable ring extensions of exponent one. He managed to extend Jacobson's correspondence for field extensions ([36]) to the setting of Galois extensions of exponent one ([68]). Namely, he proved that each intermediate subring B of a Galois extension $A \subseteq C$, such that $B \subseteq C$ is also Galois, correspond univocally to a restricted Lie subalgebra of $\mathrm{Der}_A(C)$ that is also a C-direct summand of $\mathrm{Der}_A(C)$ as C-module ([68, Theorem 13]). He also demonstrated that such an intermediate subring B satisfies also that $A \subseteq B$ is Galois ([68, Theorem 11]). Later, using homological methods, M. André characterized these intermediate subrings as those such that C is projective as a B-module ([1, Théorème 71]).

In this thesis, we focus on Galois towers of rings of fixed differential rank, that is, tower of rings $A \subseteq B \subseteq C$ such that $A \subseteq C$, $B \subseteq C$ and $A \subseteq B$ are Galois extensions of exponent one such that the C-modules $\Omega_{C/A}$ and $\Omega_{C/B}$ have constant rank. Given a Galois extension $A \subseteq C$, such that $\Omega_{C/A}$ has constant rank as C-module, we define a functor whose set of A-points is the set of Galois towers of fixed differential rank.

Definition 0.7. For a Galois extension $A \subseteq C$, such that $\Omega_{C/A}$ has constant rank n as C-module, and for a fixed integer $0 \leq r \leq n$, the *Yuan functor* associated to $A \subseteq C$ and r is the covariant functor from the category of A-algebras to the category of sets given by

$$\mathcal{Y}^r_{C/A}\colon \mathrm{Alg}_A \to \mathrm{Sets}$$
$$A' \mapsto \left\{ B' \text{ subring} : \begin{array}{l} A' \subseteq B' \subseteq C \otimes_A A' =: C', \\ B' \subseteq C' \text{ is Galois and } \Omega_{C'/B'} \text{ has rank } r \end{array} \right\}.$$

In Section 2.3 in the second chapter, we prove that this functor is representable by a quasi-projective A-scheme (Theorem 2.92) and we study some of its geometric properties (Theorem 2.95). More precisely, we prove the following result:

Theorem 0.8. *For a Galois extension $A \subseteq C$, such that $\Omega_{C/A}$ has constant rank n as C-module, an for a fixed integer $0 \leq r \leq n$, the Yuan functor $\mathcal{Y}^r_{C/A}$ is representable by a quasi-projective and smooth A-scheme that has smooth irreducible fibers of dimension $(p^n - p^{n-r})(n-r)$.*

Purely inseparable ring extensions of higher exponent

We now turn to the case of higher exponent. As we have already mentioned, purely inseparable ring extensions were introduced as *special algebras* by F. Pauer ([49]). He presented them as finite ring extensions $A \subseteq C$ of finite exponent that satisfy the following equivalent conditions:

(1) C is a projective A-module, and for each prime ideal $\mathfrak{p} \subset A$, there is a faithfully flat ring extension $A_\mathfrak{p} \to A'$ that induces an isomorphism of A'-algebras $C_\mathfrak{p} \otimes_{A_\mathfrak{p}} A' = A'[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$ for some $e_i > 0$.

(2) C is a projective A-module and for each prime ideal $\mathfrak{p} \subset A$, there are positive integers $e_1 \geq \cdots \geq e_n$ and polynomials $P_i \in A_\mathfrak{p}[X_1, \ldots, X_{i-1}]$ for $i = 1, \ldots, n$, such that $C_\mathfrak{p}$ admits a presentation as $A_\mathfrak{p}$-algebra $C_\mathfrak{p} = A_\mathfrak{p}[x_1, \ldots, x_n]$ with defining relations $x_i^{p^{e_i}} = P_i(x_1^{p^{e_i}}, \ldots, x_{i-1}^{p^{e_i}})$ for $i = 1, \ldots, n$.

(3) The module of differentials $\Omega_{A[C^{p^e}]/A}$ is a projective $A[C^{p^e}]$-module for all $e \geq 0$.

In some sense, these equivalences can be seen as a generalization to the higher exponent setting of the equivalences (1)⇔(2)⇔(4) from Theorem 0.6 that summarizes the characterizations of purely inseparable extensions of exponent one.

Later, P. Sancho de Salas studied the notion of *differentially homogeneous algebra*, that is, an A-algebra C that is flat, of finite presentation, and such that the module of principal parts $\mathrm{P}^k_{C/A}$ is projective over C for all $k \geq 0$. He proved in [56] that purely inseparable extensions are differentiably homogeneous algebras that have finite exponent. In other words, he proved that for a finite ring extension $A \subseteq C$ of finite exponent, the following condition is also equivalent to the three properties stated above:

(4) The C-module of principal parts $\mathrm{P}^k_{C/A}$ is projective for all $k \geq 0$.

In this thesis, we enlarge the above list of equivalences using differential operators. In Section 3.2 in the third chapter, we prove a result on extensions of differential operators (Proposition 3.39), which allows us to state a new characterization of purely inseparable extensions in terms of some modules of differential operators. As a combination of Proposition 3.47 and Proposition 3.43, we obtain a characterization for purely inseparable extensions that generalizes Theorem 0.5 to the higher exponent setting as follows:

Theorem 0.9. *Let $A \subseteq C$ be a finite ring extension of finite exponent. Then $A \subseteq C$ is purely inseparable if and only if C is a projective $A[C^{p^e}]$-module for all $e \geq 0$, and the module of differential operators $\mathrm{Diff}^{p^e}_A(C)$ is a C-module direct summand of $\mathrm{End}_A(C)$ for all $e \geq 0$.*

In addition, using techniques on differential operators, we re-obtain from a different perspective the characterization in terms of the modules of principal parts corresponding to property (4) above. In conclusion, we can summarize the characterizations of purely inseparable ring extensions in the next theorem:

Theorem 0.10. *For a finite ring extension $A \subseteq C$ of finite exponent, the following are equivalent:*

(1) $A \subseteq C$ is purely inseparable (as in Definition 0.3).

(2) C is a projective A-module and for each prime ideal $\mathfrak{p} \subset A$, the ring extension $A_\mathfrak{p} \subseteq C_\mathfrak{p}$ has a normal generating sequence (NGS), i.e., there is a presentation $C_\mathfrak{p} = A_\mathfrak{p}[x_1, \ldots, x_n]$ with defining relations given by $x_i^{p^{e_i}} = P_i(x_1^{p^{e_i}}, \ldots, x_{i-1}^{p^{e_i}})$ for some integers $e_1 \geq \cdots \geq e_n > 0$ and polynomials $P_i \in A_\mathfrak{p}[X_1, \ldots, X_{i-1}]$, for $i = 1, \ldots, n$.

(3) The module of differentials $\Omega_{A[C^{p^e}]/A}$ is a projective $A[C^{p^e}]$-module for all $e \geq 0$.

(4) C is a projective $A[C^{p^e}]$-module and the module of differential operators $\mathrm{Diff}^{p^e}_A(C)$ is a C-module direct summand of $\mathrm{End}_A(C)$, for all $e \geq 0$.

(5) The C-module of principal parts $\mathrm{P}^{p^e}_{C/A}$ is projective for all $e \geq 0$.

Purely inseparable towers of rings

We continue with purely inseparable towers. As we have explained above, one of the main interests of the purely inseparable theory of fields is to understand the intermediate subextensions of a purely inseparable extension and to establish some correspondences between them and other subojects of another algebraic object. We are interested in the comprehension of *purely inseparable towers* of rings, that is, towers of rings $A \subseteq B \subseteq C$ such that $A \subseteq C$, $B \subseteq C$ and $A \subseteq B$ are purely inseparable extensions.

In the exponent one case, given $A \subseteq C$ a Galois extension, M. André proved that the intermediate subrings B that induce purely inseparable towers are those such that

C is projective as a B-module. However, the situation becomes more complicated in higher exponent. If $A \subseteq C$ is a purely inseparable extension of exponent greater than one and B is an intermediate subring such that C is projective as B-module, it is not true in general that $A \subseteq B$ and $B \subseteq C$ are also purely inseparable (see Example 3.52). Therefore, in this thesis, we exhibit some conditions for the intermediate subrings B of a purely inseparable extension $A \subseteq C$ which ensure that both subextensions $A \subseteq B$ and $B \subset C$ are also purely inseparable. With this purpose, we introduce the following class of ring extensions:

Definition 0.11. A finite ring extension $A \subseteq C$ of finite exponent is an *$\mathcal{F}$-extension* if C is a projective $A[C^{p^e}]$-module for all $e \geq 0$.

We note that any purely inseparable extension is in particular an $\mathcal{F}$-extension. In Section 3.3, we prove that imposing this condition to certain subextensions of a purely inseparable extension $A \subseteq C$ related to the intermediate subring B, we obtain a purely inseparable tower $A \subseteq B \subseteq C$. More precisely, what we prove that the following:

Theorem 0.12. *Let $A \subseteq C$ be a purely inseparable ring extension and B an intermediate subring such that $A \subseteq B$ and $B \subseteq C$ are $\mathcal{F}$-extensions. If $A \subseteq B[C^{p^e}]$ is an $\mathcal{F}$-extension for all $e \geq 1$, then $A \subseteq B \subseteq C$ is a purely inseparable tower.*

Using the above theorem, we obtain the next characterization for purely inseparable towers of exponent two:

Corollary 0.13. *Let $A \subset C$ be a purely inseparable ring extension of exponent two and let B be an intermediate subring. Then $A \subseteq B \subseteq C$ is a purely inseparable tower if and only if $A \subseteq B$ and $B \subseteq C$ are both $\mathcal{F}$-extensions.*

In addition, we study when the composition of two purely inseparable extensions $A \subseteq B$ and $B \subseteq C$ induce a purely inseparable tower $A \subseteq B \subseteq C$. We show that this holds if we impose some extra conditions:

Theorem 0.14. *Let $A \subseteq B$ and $B \subseteq C$ be purely inseparable extensions of rings. If $A \subset B[C^{p^e}]$ is an $\mathcal{F}$-extension for all $e \geq 0$, then $A \subset C$ is also purely inseparable.*

Lastly, as we do not understand completely purely inseparable towers of rings, we are far from obtaining a purely inseparable Galois theory for rings as the ones that have been developed in the case of fields. Nevertheless, when dealing with these extensions, we have obtained a generalization of the Jacobson-Bourbaki correspondence for intermediate subfields of any finite field extension ([38, I, §2, Theorem 2]) to the setting of certain ring extensions of any characteristic. In fact, we prove in Section 1.3 in the first chapter the following result, which applies in particular to purely inseparable extensions of rings.

Theorem 0.15. *Let $A \subseteq C$ be a finite extension of rings such that C is projective as A-module. In addition, assume that the induced morphism* $\mathrm{Spec}(C) \to \mathrm{Spec}(A)$ *is an homeomorphism. There is a bijection between the subset of subrings*

$$\mathcal{P}_{C/A} := \left\{ B : \begin{array}{l} B \text{ is an intermediate subring } A \subseteq B \subseteq C \\ \text{and } C \text{ is a } B\text{-projective module} \end{array} \right\} \Bigg($$

and the subset of subalgebras

$$\mathcal{D}_{C/A} := \left\{ H : \begin{array}{l} H \text{ is an unital } A\text{-subalgebra of } \mathrm{End}_A(C) \text{ and} \\ \text{a direct summand of } \mathrm{End}_A(C) \text{ as } C\text{-module} \end{array} \right\} \Bigg($$

given by the following inverse maps

$$\begin{array}{cccc} \mathcal{P}_{C/A} & \to \mathcal{D}_{C/A}, & \mathcal{D}_{C/A} & \to \mathcal{P}_{C/A} \\ B & \mapsto \mathrm{End}_B(C) & H & \mapsto B_H := \{x \in C : [\varphi, x] = 0,\ \forall \varphi \in H\}. \end{array}$$

Modular extensions of rings

We have mentioned above that there is a subclass of purely inseparable extensions of fields that is particularly interesting, namely, modular extensions. In this thesis, we extend the original notion of modular extension of fields to the setting of rings. Following one of the characterizations of M. E. Sweedler ([62, Theorem 1]) and using a notion of generalized p-basis introduced by S. Yuan ([67]), we define a modular extension of rings as:

Definition 0.16. A finite extension of rings $A \subseteq C$ is a *modular extension* if

(1) $A \subseteq C$ has finite exponent, i.e., $C^{p^e} \subseteq A$ for some $e \geq 0$;

(2) C is a projective A-module; and

(3) for each prime ideal $\mathfrak{p} \subset A$, the extension $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}}$ has a generalized p-basis, i.e., there is an isomorphism of $C_{\mathfrak{p}} \simeq A_{\mathfrak{p}}[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}} - a_1, \ldots, X_n^{p^{e_n}} - a_n \rangle$ $A_{\mathfrak{p}}$-algebras for some $a_i \in A_{\mathfrak{p}}$ and $e_i > 0$.

In Section 4.2 in the fourth chapter, we show that any modular extension of rings is purely inseparable (Proposition 4.33). We also characterize them among purely inseparable extensions as those which satisfy a condition on linearly disjointedness (Theorem 4.38), as it occurs in the setting of fields. More precisely, our final result is:

Theorem 0.17. *Let $A \subseteq C$ be a finite ring extension of finite exponent. Then $A \subseteq C$ is modular if and only if $A \subseteq C$ is purely inseparable, and C^{p^e} and A are linearly disjoint for all $e \geq 0$.*

Some open questions

As one might note, the topic of purely inseparable extensions of rings is not exhausted and some natural questions arise. We include here some of these questions on which we hope to work in the future.

Differentiably simple rings and higher exponent extensions. We recall that a ring R is differentiably simple if the only ideals $I \subseteq R$ such that $D(I) \subseteq I$ for any derivation $D\colon R \to R$ are 0 and R. As we review in Subsection 2.1.4 in the second chapter, L. R. Harper proved that any Noetherian differentiably simple ring A of characteristic p has a presentation $A \simeq K[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$ for some coefficient field K. Using this notion of differentiably simple, purely inseparable extensions of exponent one can

be characterized as finite ring extensions $A \subseteq C$ of exponent one such that C is a projective A-module and $C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ is differentiably simple for each prime ideal $\mathfrak{p} \subset A$. Continuing with the work of S. Yuan in [67], it is natural to ask if this characterization can be extended to the higher exponent setting, that is, if one can define a similar notion of differentiably simple rings using higher derivations or differential operators of higher order that allows us to characterize purely inseparable extensions of greater exponent and such that there is an analogue of Harper's structure theorem.

A Galois correspondence for purely inseparable towers of rings. In the exponent one case, we know that the intermediate subrings B of a Galois exponent one extension such that both $A \subseteq B$ and $B \subseteq C$ are also Galois, are those such that C is a projective B-module. We also know that these intermediate subrings are in a one-to-one correspondence with certain Lie subalgebras of $\mathrm{Der}_A(C)$. For the higher exponent case, we have found sufficient conditions for an intermediate subring B of a purely inseparable ring extension $A \subseteq C$ to induce a purely inseparable tower $A \subseteq B \subseteq C$. We would like to find the necessary conditions for the intermediate subrings to make this situation occurs. In other words, we want to characterize all the intermediate subrings B of a purely inseparable ring extension $A \subseteq C$ such that $A \subseteq B \subseteq C$ is a purely inseparable tower. Moreover, if one could obtain such a characterization, one would also want to work in two more directions. On the one hand, to establish a correspondence between those subrings and other subobjects of an algebraic object, which generalizes the already known Yuan's correspondence for exponent one. On the other hand, to define a representable functor, as Yuan's functor for the exponent one case (see Definition 0.7), which parametrizes those intermediate subextensions.

Modular extensions and differential operators. It is clear that differential operators play an important role in the study of purely inseparable extensions. The recent results of M. Wechter [64] show that they have also a relation with modular extensions of fields. We want to understand this relation and, if possible, to generalize it to the setting of rings. That is, we would like to obtain a characterization of modular extensions of rings using differential operators.

Summary of contents

The thesis is organized in four chapters, which contain all the results explained before, and a short appendix, which collects some basic results of Commutative Algebra that are used systematically through the thesis.

Chapter 1 is dedicated to projective modules. We give a brief introduction to these algebraic structures, in particular, to finite extensions of rings $A \subseteq C$ such that C is projective as A-module. We review some basics properties that will be used frequently through the thesis. We also focus on some intermediate subextensions of finite projective extensions of rings. In this context, we prove the generalization of the Jacobson-Bourbaki correspondence established in Theorem 0.15.

Chapter 2 studies purely inseparable ring extensions of exponent one, or Galois extensions (see Definition 0.4). We include here some preliminaries on derivations, Kähler differentials, p-basis and differentiably simple rings, which are concepts that

are used to characterize Galois extensions. Considering derivations as differential operators of order one, we prove Theorem 0.5 that gives a new characterization for these extensions. Moreover, we review Galois towers of rings and define the Yuan functor as in Definition 0.7. We prove Theorem 0.8 on the representability of the Yuan functor by an scheme and study its geometric properties.

Chapter 3 is devoted to purely inseparable extensions of rings in general (Definition 0.3). We first review the original characterizations given by F. Pauer in terms of normal generating sequences and modules of differentials. Then we study these extensions from the perspective of differential operators and obtain the new characterization in Theorem 0.9. We also use these techniques on differential operators to re-obtain a characterization involving the modules of principal parts. In conclusion, we obtain Theorem 0.10. In addition, we study purely inseparable towers of rings and provide some sufficient conditions for a tower of rings $A \subseteq B \subseteq C$ to be purely inseparable. These conditions are condensed in Theorem 0.12, Corollary 0.13 and Theorem 0.14.

Chapter 4 addresses modular extensions of rings. We begin with some preliminaries on linearly disjointedness and generalized p-basis. Then, we use them to extend the original definition of modular extensions of fields to the setting of rings (Definition 0.16). We prove that these extensions are exactly the purely inseparable ring extensions that satisfy certain conditions on linearly disjointedness as in Theorem 0.17.

To ease the reading, we include also at the beginning of each chapter a short introduction and an overview of the organization of the sections.

Notation and conventions

In this thesis, all the rings are assumed to be commutative and with unity, unless otherwise stated. If no explicit mention is made, we assume that the rings can be of any characteristic. In other case, it will be specified at the beginning of the section. Throughout, p denotes a rational prime.

The set of prime ideals of a ring R is denoted by $\mathrm{Spec}(R)$. In fact, it is a topological space under the *Zariski topology*, whose basic open subsets are of the form $\{\mathfrak{p} \in \mathrm{Spec}(R) : x \notin \mathfrak{p}\}$ for $x \in R$.

A ring R is *local* if it has only one maximal ideal. In this case, we denote by $\mathfrak{m}_R$ its maximal ideal and by $\kappa(R) := R/\mathfrak{m}_R$ its *residue field*. We usually write $(R, \mathfrak{m}_R)$ to refer to such a ring.

We denote by Sets and Groups the categories of sets and groups. Given a ring A, we denote by Alg_A the category of A-algebras, where an object $A' \in \mathrm{Alg}_A$ is a ring together with a ring homomorphism $A \to A'$ and an arrow between two objects $A', A'' \in \mathrm{Alg}_A$ is an A-linear homomorphism of rings $\varphi\colon A' \to A''$.

We note that there is also a more general notion of algebra over a commutative ring, that will be used punctually in some sections, for example when dealing with endomorphisms (see discussion 1.22). Given R a commutative ring with unity, an

associative algebra is a (non necessarily commutative) ring H whose center contains R and that has also an structure of R-module. Since H is assumed to have an identity element, these algebras are sometimes called *unital associative algebras*. When H is assumed to be commutative, it is said to be a *commutative algebra* over R. In this case, H is simply a ring together with an homomorphism of rings $R \to H$, as we stated in the previous paragraph. However, whether or not H is commutative, we will simply say that H is an R-algebra when the context is clear.

CHAPTER 1
On projective modules

This chapter is dedicated to the study of projective modules. These modules are a particular case of flat modules which enlarge the class of free modules over a ring. The notion of projective module was firstly introduced by H. Cartan and S. Eilenberg in [14]. They used it to refine the definition of the torsion functor, which originally relied on properties of free modules. They noted that using free modules was unnecessarily restrictive and that it was sufficient to use projective modules. Later, projective modules have become a relevant tool in Homological Algebra among other areas.

Our study of projective modules will follow the perspective of Commutative Algebra. We will work mostly in the context of finite ring extensions, so we are particularly interested in finitely generated projective modules. It is well-known that these modules coincide with the class of flat modules with finite presentation. We will pay special attention to those that have constant finite rank. A useful fact is that the modules with this condition can be characterized among the finitely generated modules using the Fitting ideals.

To be more precise, the objects of interest in this thesis will be finite and projective extensions of rings, that is, finite extensions of commutative rings with unity $A \subseteq C$ such that the C is projective as a module over A. As we will show, purely inseparable extensions of rings belong to this class of extensions. But from now on, in this chapter we will remain in the context of finite projective extensions of rings.

Given such an extension, one of our principal interests is to understand the intermediate subextensions of rings that are also projective. Namely, given a finite projective extension of rings $A \subseteq C$, we are interested in the intermediate subrings B, i.e., $A \subseteq B \subseteq C$, such that C is also projective as B-module. On the one hand, we show that there is a correspondence between these projective subextensions and some subalgebras of the module of endomorphisms of the extension, when $\mathrm{Spec}(A)$ and $\mathrm{Spec}(C)$ are homeomorphic. On the other hand, assuming that C has constant rank over A, we use a subfunctor of the Grassmannian functor of submodules to parametrize the intermediate projective subextensions of constant rank.

Organization. This chapter contains four sections. The first two sections serve as an introduction to projective modules and finite projective ring extensions in general. They are mainly expository as they collect well-known results that can be found

in classic textbooks of algebra. The last two sections are devoted to the study of projective intermediate subextensions of a finite projective extension of rings. The results included here were obtained by the author of this thesis in collaboration with D. Sulca and partially with O. Villamayor. In particular, the contents from the third section can be found mainly in [11, §5], while the contents from the last section come from [12].

Section 1.1 reviews the notion of projective module and some characterizations and basic properties of these modules. We emphasize here on finite projective modules, particularly on those with constant rank.

Section 1.2 focuses on finite projective ring extensions. We set up some properties for finite ring extensions $A \subseteq C$ such that C is projective over A as a module, and for the intermediate subrings $A \subseteq B \subseteq C$ such that C is also projective as B-module.

Section 1.3 establishes a generalization of Jacobson-Bourbaki correspondence for finite field extensions to the setting of finite projective extensions with homeomorphic spectra. More accurately, given a finite ring extension $A \subseteq C$ such that C is projective over A and the induced map between the spectra $\mathrm{Spec}(A)$ and $\mathrm{Spec}(C)$ is an homeomorphism, we prove that each intermediate subring $A \subseteq B \subseteq C$ such that C is projective over B corresponds univocally to a unital A-subalgebra of $\mathrm{End}_A(C)$ that is also a direct summand as left C-submodule (Theorem 1.30).

Section 1.4 introduces a parametrization for the projective subextensions of fixed rank of a finite projective extension of rings with constant rank. More precisely, given a finite projective ring extension $A \subseteq C$ of constant rank m and given a positive integer q such that $q|m$, we define a subfunctor of the Grassmannian functor of submodules, which turns out to be representable by an scheme over A, whose set of A-points is formed by the subrings $A \subseteq B \subseteq C$ such that C is projective of rank q over B (Theorem 1.36).

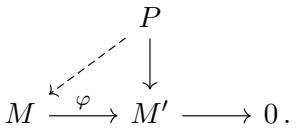
1.1. Preliminaries on projective modules

In this section, we review some preliminaries on projective modules. We focus specially on the study of finite projective modules. Most of the material included here is available at classical books of Algebra, see [14, I and II] for projective modules in general and see [9, II, §5] for finite projective modules.

We begin by recalling the definition of projective module over a ring. We warn the reader that the original definition from H. Cartan and S. Eilenberg was for a module over a ring, not necessarily commutative, with unity. However, we shall restrict ourselves to the case of commutative rings. Therefore, through all the chapter, the rings are assumed to be commutative of any characteristic and with unity. In particular, in what follows, A denotes such a ring.

Definition 1.1 ([14, I, §2])**.** An A-module P is *projective* if for every surjection of A-modules $\varphi\colon M \to M'$ the map $\mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, M')$ derived from φ is surjective, i.e., if for each homomorphism $P \to M'$ there exists an homomorphism

$P \to M$ such that the following diagram commutes:



Note that this definition is equivalent to say that an A-module P is projective if the functor $\mathrm{Hom}_A(P, -)$ of the category of A-modules is exact ([14, II, §4, Proposition 4.6]). Indeed, the condition on Definition 1.1 asks $\mathrm{Hom}_A(P, -)$ to be right exact and we already know that it is left exact ([14, II, §4, Proposition 4.4]).

Projective modules admit some interesting characterizations that will be used frequently in this thesis. We collect these well-known equivalent conditions in the next proposition.

Proposition 1.2 ([14, I, §2, Theorem 2.2 and Proposition 2.4])**.** *Let P be an A-module. The following statements are equivalent:*

(1) P is a projective A-module.

(2) P is a direct summand of a free A-module.

(3) Every exact sequence of A-modules $0 \to M \to N \to P \to 0$ splits.

In particular, every free module and every direct summand of a projective module is projective.

We exhibit now some relevant properties of projective modules related to the tensor product operation. We recall first that the tensor product of projective modules is projective again.

Proposition 1.3 ([14, II, §5, Proposition 5.3])**.** *Let P and P' be projective A-modules. Then $P \otimes_A P'$ is also a projective A-module.*

The following proposition formalizes that projectivity is preserved under base change and descends along faithfully flat ring maps. The permanence of projectivity by base change is a direct consequence of the above characterization and the fact that direct sums commute with tensor products ([8, §4.1, Proposition 8]). The proof of the faithfully flat descent of the projectivity is more complicated. It was originally stated by M. Raynaud and L. Gruson in [27], but the proof contained a mistake that was rectified later by A. Perry in [50].

Proposition 1.4. *Let $A \to A'$ be an homomorphism of rings and let P be an A-module.*

(1) If P is projective, then $P \otimes_A A'$ is a projective A'-module.

(2) If $A \to A'$ is faithfully flat and $P \otimes_A A'$ is a projective A'-module, then P is projective as A-module.

The first statement in the previous proposition tells us that projectivity is preserved by extension of scalars ([14, II, §6, Proposition 6.1]). The same does not hold for restriction of scalars in general. However, it holds for restriction of scalars by projective morphisms, as it is expressed in the next proposition.

Proposition 1.5 ([14, II, §6, Proposition 6.2]). *Let $A \to A'$ be a ring homomorphism such that A' is projective as A-module. If P is a projective A'-module, then the A-module P obtained by restriction of scalars is also projective.*

We shall draw special attention to finitely generated projective modules. These modules can be characterized by properties as having finite presentation and being flat or being locally free, as set out in the next proposition.

Definition 1.6. An A-module P is *locally free of finite rank* if for every prime ideal $\mathfrak{p} \subset A$, there is $f \in A \setminus \mathfrak{p}$ such that $M_f := M \otimes_A A_f$ is a finitely generated free A_f-module.

Proposition 1.7 ([9, II, §5.2, Theorem 1 and Corollary 2]). *For an A-module P, the following conditions are equivalent:*

(1) P is finitely generated and projective.

(2) P is locally free of finite rank.

(3) P is flat of finite presentation.

(4) P has finite presentation and $P_\mathfrak{p} := P \otimes_A A_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module for every prime ideal $\mathfrak{p} \subset A$.

Remark 1.8. It is easy to deduce from the above characterization that any finitely generated projective module over a local ring is finite free (see [47, 1, §2, Theorem 2.5]). Indeed, I. Kaplansky proved in [39] that any projective module, not necessarily finite, over a local ring is free.

Remark 1.9. Being flat and having finite presentation are properties that ascend by base change and descend by faithfully flat morphisms (see Proposition A.15 and Proposition A.26). Thus if P is a finite projective A-module, then for any ring homomorphism $A \to A'$, the A'-module $P' := P \otimes_A A'$ is also finite and projective. Conversely, if $A \to A'$ is faithfully flat and P' is finite projective over A', then P is also finite and projective as A-module.

We show that the dual of a module preserves the condition of being finitely generated and projective.

Proposition 1.10. *Let P be a finitely generated projective A-module. Then the dual module $P^* := \mathrm{Hom}_A(P, A)$ is also a finitely generated projective A-module. In addition, P is naturally isomorphic to its double dual P^{**}.*

Proof. Since P is finitely generated and projective, there exists a positive integer m and an A-module P' such that $P \oplus P' = A^m$. Recall that any finite free module is isomorphic to its dual (Proposition A.33). Thus, we have

$$A^m \simeq \mathrm{Hom}_A(A^m, A) \simeq \mathrm{Hom}_A(P \oplus P', A) \simeq \mathrm{Hom}_A(P, A) \oplus \mathrm{Hom}_A(P', A) = P^* \oplus P'^*.$$

It follows from these isomorphisms that P^* is finitely generated and projective as A-module. The final claim follows from the local characterization of finite projective modules (Proposition 1.7) and the already mentioned fact that any finite free module is naturally isomorphic to its double dual (Proposition A.33). □

Remark 1.11. Proposition 1.10 does not hold in general without the assumption of finiteness. For example, consider the $\mathbb{Z}$-module $M := \oplus_{n\in\mathbb{N}}\mathbb{Z}$. It is free and, in particular, projective. However, its dual module $M^* = \prod_{n\in\mathbb{N}}\mathbb{Z}$ is not projective over $\mathbb{Z}$ (see [45, 1, §2, Exercise 2.6]).

1.12. *Rank of a finite projective module.* Let P be a finitely generated projective A-module. For each prime ideal $\mathfrak{p} \subset A$, the rank of the $A_\mathfrak{p}$-module $P_\mathfrak{p}$, that is, the minimal number of generators of $P_\mathfrak{p}$ as free $A_\mathfrak{p}$-module, is called the *rank* of P at $\mathfrak{p}$. Recall that, by the local version of Nakayama's Lemma (see Corollary A.35), this rank coincides with the dimension of $P \otimes_A \kappa(\mathfrak{p})$ as $\kappa(\mathfrak{p})$-vector space, where $\kappa(\mathfrak{p}) := A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is the residue field at $\mathfrak{p}$. If the rank of P at every $\mathfrak{p} \in \mathrm{Spec}(A)$ is equal to m, then P is said to have *(constant) rank* m. Note that if P has finite rank m as A-module, then $P \otimes_A A'$ has the same rank as A'-module for any ring homomorphism $A \to A'$ ([9, §5.3, Proposition 4]).

Finite projective modules of constant rank are closely related to Fitting ideals. In fact, these ideals, which were originally introduced by H. Fitting in [21], encode many structural properties of modules. We give now the definition of Fitting Ideals and recall some basic properties that will be used later. These results and a more detailed introduction on this topic can be found in [44, Appendix D].

1.13. *Fitting ideals.* Let M be a finitely generated A-module and let $t_1, \ldots, t_n$ be a system of generators of M. Let the exact sequence $0 \to N \to A^n \xrightarrow{\varphi} M \to 0$ be the *presentation of M defined by* $\{t_1, \ldots, t_n\}$, where φ sends each element e_i of the standard basis of A^n into t_i, for all $i = 1, \ldots, n$. The kernel $N = \ker(\varphi)$ admits a system of generators $\{u_\lambda\}_{\lambda\in\Lambda}$ where $u_\lambda = (x_1^{(\lambda)}, \ldots, x_n^{(\lambda)}) \in A^n$ and then the *relation matrix* of M with respect to $\{t_1, \ldots, t_n\}$ is defined as $(x_i^{(\lambda)})_{i=1,\ldots n,\lambda\in\Lambda}$. For $1 \le i \le n$, we denote by $F_i(M)$ the ideal of A generated by all $(n-i)$-rowed subdeterminants of this relation matrix. We set $F_i(M) := A$, for $i > n$, and $F_i^A(M) := 0$, for $i < 0$. It can be proved that these ideals $F_i(M)$ do not depend on the special choice of the relation matrix of M with respect to $\{t_1, \ldots, t_n\}$ nor on the choice of the system of generators for M ([44, Lemma D.1 and Lemma D.2]). Thus, these ideals are intrinsic to the A-module M.

We define $\mathrm{Fitt}_i^A(M) := F_i(M)$ as the *i-th Fitting ideal* of the A-module M. When the base ring A is clear, we simply write $\mathrm{Fitt}_i(M)$. By construction, we have the following inclusions

$$0 \subseteq \mathrm{Fitt}_0(M) \subseteq \mathrm{Fitt}_1(M) \subseteq \cdots \subseteq A.$$

The Fitting ideals behave well by base change, that is, for any ring homomorphism $A \to A'$, the Fitting ideal $\mathrm{Fitt}_i^{A'}(M \otimes_A A')$ coincides with $A' \cdot \mathrm{Fitt}_i^A(M)$, the extended ideal of $\mathrm{Fitt}_i^A(M)$ under $A \to A'$ (see [44, Rules D.4]). In particular, this property applies for localization at any multiplicatively closed subset.

As it shows the following characterization, the Fitting ideals will be our main tool to detect whether a finitely generated module is projective of a fixed rank.

Proposition 1.14. *Let P be a finitely generated A-module. Then P is projective of constant rank m if and only if the following equivalent conditions hold:*

(1) $\mathrm{Fitt}_i(P) = 0$, *for* $i < m$, *and* $\mathrm{Fitt}_m(P) = A$.

(2) $\mathrm{Fitt}_{m-1}(P) = 0$ *and* $\mathrm{Fitt}_m(P) = A$.

Proof. The first equivalence is [44, Corollary D.13]. The second equivalence follows from the fact that $\mathrm{Fitt}_i(M) \subseteq \mathrm{Fitt}_{i+1}(M)$ for all $i \in \mathbb{Z}$. □

1.2. Projective ring extensions

In this section, we collect some properties that hold for finite ring extensions $A \subseteq C$ such that C is a projective A-module. The results in here are developed in [12, §4.1].

Lemma 1.15. *Let $A \subseteq C$ be a finite extension of rings. If C is projective as A-module, then the quotient C/A is also projective as A-module and, thus, the sequence $0 \to A \to C \to C/A \to 0$ is split exact.*

Proof. Since $A \subseteq C$ is a finite extension, we have that C is finitely generated as A-module and projective by hypothesis. Then by Proposition 1.7, we have that $C_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module of finite rank for each $\mathfrak{p} \in \mathrm{Spec}(A)$. As a consequence of Nakayama's Lemma (see Proposition A.36), a basis for $C_\mathfrak{p}$ as $A_\mathfrak{p}$-module can be obtained by lifting any basis for $C_\mathfrak{p}/\mathfrak{p}C_\mathfrak{p}$ over $\kappa(\mathfrak{p})$. Note that we can always choose a basis for this vector space that contains the vector corresponding to the identity element 1. Hence there is a basis for $C_\mathfrak{p}$ over $A_\mathfrak{p}$ containing 1. This implies that $A_\mathfrak{p}$ is a direct summand of $C_\mathfrak{p}$ and thus the quotient $(C/A)_\mathfrak{p} = C_\mathfrak{p}/A_\mathfrak{p}$ is free of finite rank as $A_\mathfrak{p}$-module. Finally, it is clear that A is finitely generated as A-module, and C is finitely presented as A-module by Proposition 1.7. Then it follows by Proposition A.25.(4) that C/A is also finitely presented. Therefore, using the characterization in Proposition 1.7, we conclude that C/A is a projective A-module and, as a consequence, the exact sequence $0 \to A \to C \to C/A \to 0$ splits. □

Remark 1.16. Note that any finite extension of rings $A \subseteq C$, such that C is projective over A, is faithfully flat. In fact, by Lemma 1.15, we know that the quotient C/A is also projective as A-module. Thus, $A \to C$ is an injective morphism such that both C and C/A are flat A-modules. Therefore, by Proposition A.18, the map $A \to C$ is faithfully flat. Moreover, for any ring homomorphism $A \to A'$, the base change $A' \to C' := C \otimes_A A'$ is also a finite extension of rings such that C' is projective over A'. Indeed, by Proposition A.16, we know that $A' \to C'$ is also faithfully flat. So, in particular, it is injective and we can write $A' \subseteq C'$. The condition of being finite and projective follows by Remark 1.9. In addition, if C has constant rank over A, then C' has the same rank over A' (see discussion 1.12.)

The following lemmas collect some properties of ring towers $A \subseteq B \subseteq C$ where C is a projective module over A. The proof of the next lemma uses the fact that any finitely generated projective module of constant rank over an Artinian ring is free, which follows from a more general result of J.-P. Serre ([59, Théorème 1]).

Lemma 1.17. *Let $A \subseteq C$ be a finite extension of rings such that C is a projective A-module. Fix B an intermediate subring, $A \subseteq B \subseteq C$, such that C is a projective B-module. Then B and C/B are finitely generated projective as A-modules. Moreover, if C has rank m as A-module and rank q as B-module. Then*

(1) $q|m$ and B has rank $\frac{m}{q}$ over A.

(2) The quotient module C/B has rank $m - \frac{m}{q}$ over A.

Proof. We assume first that C is a finitely generated projective A-module and that it is also projective as B-module. By Lemma 1.15, we know that B is a direct summand of C as a B-module. Thus B and C/B are also A-direct summands of the finitely generated and projective A-module C. By Proposition 1.2, this implies that both B and C/B are also finitely generated projective A-modules.

In addition, we assume now that C has constant rank m over A and constant rank q over B. We claim that B has rank s over A with $qs = m$. By the discussion in 1.12, we may assume that A is a field after tensoring with $\kappa(\mathfrak{p})$ for some $\mathfrak{p} \in \mathrm{Spec}(A)$. So m is the dimension of C as A-vector space and $C \cong A^m$. Let s be the dimension of B over A, then $B \cong A^s$ as A-vector spaces. Note that B is an Artinian ring, since it is an A-algebra of finite dimension as vector space over a field (see Proposition A.4). In addition, C is a finitely generated projective B-module of constant rank q. Therefore, by the observation made above, $C \cong B^q$ as B-modules. Finally, we conclude that $A^m \cong C \cong B^q \cong (A^s)^q$, which implies $m = qs$. It is clear now that $s = \frac{m}{q}$ and C/B has rank $m - s$ over A. □

Lemma 1.18. *Let $A \subseteq C$ be a finite extension of rings such that C is a projective A-module. Let B be an intermediate subring, $A \subseteq B \subseteq C$, such that B is finitely generated as A-module. If C is flat as a B-module, then C is a finitely generated projective B-module.*

Proof. Note that B is finitely generated as A-module. Then, by Proposition A.27, we know that C has finite presentation as B-module. Thus, C is a flat B-module of finite presentation. By Proposition 1.7, we conclude that C is a finitely generated projective B-module. □

Remark 1.19. Let $A \to A'$ be any ring homomorphism. Just as we noted in Remark 1.16, any tower of rings $A \subseteq B \subseteq C$ such that C is finite and projective over both A and B is transformed by base change into a tower of rings $A' \subseteq B \otimes_A A' \subseteq C \otimes_A A'$ with the same properties. Moreover, if C has fixed rank over A and B respectively, then $C \otimes_A A'$ has the same ranks over A' and $B \otimes_A A'$ respectively (see discussion 1.12).

Some arguments concerning finite extensions $A \subseteq C$ can be simplified when A is Noetherian. In particular, when we deal with some subfunctors of the Grassmannian functor in Section 1.4, the following result will be useful to reduce the situation to the Noetherian case.

Lemma 1.20. *Let $A \subseteq C$ be a finite extension of rings. If C is projective of rank m as A-module, then there is a Noetherian subring $A_0 \subseteq A$ and a ring extension $A_0 \subseteq C_0$ such that C_0 is finitely generated projective of rank m as A_0-module and $C = C_0 \otimes_{A_0} A$.*

Proof. Since C is a finitely presented as A-module, it is a finite A-algebra of finite presentation (see discussion A.40). We can express A as the inductive limit of its Noetherian $\mathbb{Z}$-subalgebras and apply Proposition A.42 to obtain a Noetherian subring A_0' of A and a finite A_0'-algebra C_0' such that $C_0' \otimes_{A_0'} A = C$. In addition, C_0' is an A_0'-module of finite presentation because A_0' is Noetherian (see discussion A.23).

Recall that C is projective of rank m as A-module, so we have by Proposition 1.14 that $\mathrm{Fitt}_{m-1}^{A}(C) = 0$ and $\mathrm{Fitt}_{m}^{A}(C) = A$. Using that $\mathrm{Fitt}_{m}^{A_0'}(C_0')A = \mathrm{Fitt}_{m}^{A}(C) = A$, we find elements $f_1, \ldots, f_s \in \mathrm{Fitt}_{m}^{A_0'}(C_0')$ and $h_1, \ldots, h_s \in A$ such that $f_1h_1 + \cdots + f_sh_s = 1$. We define A_0 as the A_0'-subalgebra of A generated by $h_1, \ldots, h_s$. We set $C_0 := C_0' \otimes_{A_0'} A_0$. Observe that C_0 is an A_0-module of finite presentation, because C_0' has finite presentation over A_0' (see Proposition A.26).

Finally, we prove that the homomorphism $A_0 \to C_0$ satisfies the required conditions. It only lefts to show that C_0 is a projective A_0-module of rank n, as this implies in particular that the map $A_0 \to C_0$ is injective. In order to prove it, we use again the characterization involving Fitting ideals from Proposition 1.14. On the one hand, $\mathrm{Fitt}_{m}^{A_0}(C_0) = \mathrm{Fitt}_{m}^{A_0'}(C_0')A_0$, and this is equal to A_0 by the way in which we have constructed A_0. On the other hand, $0 = \mathrm{Fitt}_{m-1}^{A}(C) = \mathrm{Fitt}_{m-1}^{A_0'}(C_0')A$, so $\mathrm{Fitt}_{m-1}^{A_0'}(C_0') = 0$ as A_0 is a subring of A. Hence, $\mathrm{Fitt}_{m-1}^{A_0}(C_0) = \mathrm{Fitt}_{m-1}^{A_0'}(C_0')A_0 = 0$. Thus, we conclude that C_0 is a projective A_0-module of rank m. □

1.3. Generalization of the Jacobson-Bourbaki Theorem

In this section, the algebras may not be commutative or unital. The results on this section correspond to the content in [11, §5]. Our aim is to generalize the classical Jacobson-Bourbaki correspondence for finite field extensions to the setting of certain finite extensions of commutative rings.

Theorem 1.21 (Jacobson-Bourbaki correspondence, [38, I, §2, Theorem 2])**.** *Let $K \subseteq L$ be a finite extension of fields. Then there is a bijection between the subfields E such that $K \subseteq E \subseteq L$ and the unital K-subalgebras of $\mathrm{End}_K(L)$ that are also left vector L-spaces.*

Originally, this correspondence stems from the purpose of N. Jacobson of extending the classical Galois theory to field extensions that need not be normal or separable

([34], [35]). With this aim, he stated such a correspondence for finite purely inseparable field extensions of exponent one between the subfields E of such an extension $K \subseteq L$ and the restricted Lie subalgebras of the module of derivations $\mathrm{Der}_K(L)$ ([36]). Recently, a generalization of this correspondence has been formulated by L. Brantner and J. Waldron for purely inseparable field extensions of greater exponent using methods of derived algebraic geometry ([10]). We will deepen these type of correspondences between derivations and subextensions for purely inseparable ring extensions of exponent one in Subsection 2.3.1 in the second chapter of the thesis, but from the time being we will remain in a more general setting of finite extensions.

The original correspondence from N. Jacobson for purely inseparable extensions of exponent one was quickly extended to the non-commutative case of division rings by him ([37]) and by H. Cartan ([13]) who gave the credit of the result to N. Bourbaki. This is the reason because the correspondence is called the Jacobson-Bourbaki correspondence. Later on, a similar correspondence was formulated for some intermediate subfields, called Galois subfields, of a commutative ring ([65]) and recently this formulation has been expanded to the setting of the some intermediate subfields of non-commutative rings which are finitely generated over their centers ([20]). Now, we provide a generalization of the Jacobson-Bourbaki correspondence for projective intermediate subrings of a finite projective extension of commutative rings with homeomorphic spectra.

Given a finite ring extension $A \subseteq C$ such that C is projective as A-module, we are interested in the study of the intermediate subrings $A \subseteq B \subseteq C$ such that C is also projective as B-module. When this situation occurs, B is also projective as A-module (Lemma 1.17). We want to establish a correspondence, generalizing the Jacobson-Bourbaki, between those subrings and some subalgebras of the module of endomorphisms in the case in which A and C have homeomorphic spectra. More precisely, we prove that if $A \subseteq C$ is a finite ring extension such that C is projective as A-module and $\mathrm{Spec}(A)$ and $\mathrm{Spec}(C)$ are homeomorphic via the map induced by the inclusion $A \subseteq C$, then there is a one-to-one correspondence between the intermediate subrings $A \subseteq B \subseteq C$ such that C is projective over B and the unital A-subalgebras of $\mathrm{End}_A(C)$ that are also direct summands as left C-submodules.

We begin by introducing some preliminaries on the module endomorphisms of a ring extension.

1.22. *Module endomorphisms of a ring extension.* Let $A \subseteq C$ be a ring extension, so C has a natural structure of A-module. We denote by $\mathrm{End}_A(C)$ the set of *endomorphisms* of C as A-module. Indeed, $\mathrm{End}_A(C)$ has a natural structure as left C-module as follows: if $\varphi \in \mathrm{End}_A(C)$ and $c \in C$, we define $c \cdot \varphi$ as $(c \cdot \varphi)(x) = c \cdot \varphi(x)$ for every $x \in C$. Note that under this structure, we can identify each element $c \in C$ with the multiplication map given by $x \mapsto c \cdot x$ for each $x \in C$. So we can consider $C \subseteq \mathrm{End}_A(C)$ as a submodule. We have also a natural isomorphism of left C-modules

$$\mathrm{End}_A(C) \cong \mathrm{Hom}_C(C \otimes_A C, C) =: (C \otimes_A C)^*. \tag{1.22.1}$$

that assigns to each $\varphi \in \mathrm{End}_A(C)$ a unique C-linear map $\phi\colon C \otimes_A C \to C$ such that $\phi(1 \otimes x) = \varphi(x)$ for each $x \in C$, where $C \otimes_A C$ is viewed as a left C-module.

Moreover, $\mathrm{End}_A(C)$ is also a unital non-commutative A-algebra under composition. Given $\varphi, \phi \in \mathrm{End}_A(C)$, we define the bracket

$$[\varphi, \phi] := \varphi \circ \phi - \phi \circ \varphi.$$

Note that, as an A-algebra, $\mathrm{End}_A(C)$ is closed under the bracket operation. The set of elements $x \in C$ such that $[\varphi, x] = 0$ for all $\varphi \in \mathrm{End}_A(C)$ is a subring of C, since

$$[\varphi, x+y] = [\varphi, x] + [\varphi, y] \quad \text{and} \quad [\varphi, xy] = [\varphi, x] \circ y + x \circ [\varphi, y] \quad \text{for all } x, y \in C.$$

It is called the *ring of constants* of $\mathrm{End}_A(C)$, since it coincides with the set of elements $x \in C$ such that $\varphi(xc) = x \cdot \varphi(c)$ for all $c \in C$ and $\varphi \in \mathrm{End}_A(C)$.

We study now the module of endomorphisms of a finite projective extension of rings.

Proposition 1.23. *Let $A \subseteq C$ be a finite extension of rings such that C is projective as A-module. Then*

(1) $\mathrm{End}_A(C)$ is a finitely generated projective (left) C-module.

(2) A coincides with the ring of constants of $\mathrm{End}_A(C)$, i.e.,

$$A = \{x \in C : [\varphi, x] = 0,\ \forall \varphi \in \mathrm{End}_A(C)\}.$$

Proof. As we noted in (1.22.1), we have an isomorphism of left C-modules

$$\mathrm{End}_A(C) \simeq (C \otimes_A C)^*.$$

Since C is finite and projective as A-module, so is $C \otimes_A C$ as C-module (see Remark 1.9). Finally by Proposition 1.10, we conclude that $(C \otimes_A C)^*$ is also projective and this implies (1).

Finally, we prove the equality in (2). Clearly, we have that $[\varphi, x] = 0$ for any $x \in A$, since $\varphi \in \mathrm{End}_A(C)$ is an A-linear map. Conversely, since C is finite and projective over the subring A, by Lemma 1.15 we have a decomposition $C = A \oplus C/A$. There is also a projection map $\phi\colon C \to A$ whose restriction $\phi|_A$ is the identity map. If $x \in C$ is such that $[\varphi, x] = 0$ for all $\varphi \in \mathrm{End}_A(C)$, then we have $\varphi(x) = x \cdot \varphi(1)$. In particular, the projection ϕ can be seen as an A-endomorphism of C whose image lies in A. Thus, we have $x = x \cdot \phi(1) = \phi(x) \in A$, as we wanted. □

We are interested in the good behaviour of the module of endomorphisms of a finite projective extension of rings under localization. This good behaviour with localizations is a direct consequence of the next lemma, since any finitely generated and projective module is flat and has finite presentation (Proposition 1.7).

Lemma 1.24 ([9, I, §2.10, Proposition 11])**.** *Let A be a ring and let M be a finitely presented A-module. Let $A \to A'$ be a flat homomorphism of rings. For any A-module N, there is a canonical isomorphism of A'-modules*

$$\mathrm{Hom}_A(M, N) \otimes_A A' \xrightarrow{\sim} \mathrm{Hom}_{A'}(M \otimes_A A', N \otimes_A A')$$

If we consider the case of a finite projective ring extension $A \subseteq C$ and we take $M = N = C$ in the above lemma, we obtain the desired property on the localization of the endomorphism module.

Corollary 1.25. *Let $A \subseteq C$ be a finite extension of rings such that C is projective as A-module. For any multiplicatively closed subset $S \subset A$, there is a canonical isomorphism of $S^{-1}A$-modules*

$$S^{-1}(\mathrm{End}_A(C)) \xrightarrow{\sim} \mathrm{End}_{S^{-1}A}(S^{-1}C).$$

Our first step to generalize the Jacobson-Bourbaki correspondence to the setting of certain ring extensions is to study the subalgebras and submodules of endomorphisms induced by intermediate subrings B of a finite projective ring extension $A \subseteq C$ such that C is also projective over B.

Proposition 1.26. *Let $A \subseteq C$ be a finite extension of rings such that C is projective as A-module. Let B be an intermediate subring, $A \subseteq B \subseteq C$, such that C is projective as B-module. Then*

(1) $\mathrm{End}_B(C)$ *is a unital A-subalgebra of* $\mathrm{End}_A(C)$.

(2) $\mathrm{End}_B(C)$ *is a direct summand of* $\mathrm{End}_A(C)$ *as C-module.*

Proof. Any B-endomorphism of C is in particular an A-endomorphism, since $A \subseteq B$. Therefore, $\mathrm{End}_B(C)$ is an A-subalgebra of $\mathrm{End}_A(C)$ that contains the same identity element, which is the identity morphism on C. This implies (1).

Now we prove (2). Since C is projective as B-module, it follows from Proposition 1.4.(1) that $C \otimes_B C$ is projective as C-module. Thus, by Proposition 1.2, the surjective map of C-modules $C \otimes_A C \to C \otimes_B C$ has a section. If we apply the $\mathrm{Hom}_C(-, C)$ functor to this map, we obtain an injective map of C-modules $\mathrm{Hom}_C(C \otimes_B C, C) \to \mathrm{Hom}_C(C \otimes_A C, C)$ that has a retraction. In particular, $\mathrm{Hom}_C(C \otimes_B C, C)$ is a direct summand of $\mathrm{Hom}_C(C \otimes_A C, C)$. As we noted in (1.22.1), we have isomorphisms

$$\mathrm{End}_A(C) \simeq \mathrm{Hom}_C(C \otimes_A C, C) \quad \text{and} \quad \mathrm{End}_B(C) \simeq \mathrm{Hom}_C(C \otimes_B C, C).$$

Therefore, we have proved that $\mathrm{End}_B(C)$ is a direct summand of $\mathrm{End}_A(C)$ as C-module, as we wanted. □

Our next step is to study the ring of constants attached to certain unital subalgebras of the module endomorphisms of a finite projective extension of rings. We will use the following technical lemma.

Lemma 1.27. *Let $A \subseteq C$ be a finite extension of rings such that C is a projective A-module and the induced morphism* $\mathrm{Spec}(C) \to \mathrm{Spec}(A)$ *is a homeomorphism. Let $H \subseteq \mathrm{End}_A(C)$ be a C-module direct summand. Given a prime ideal $\mathfrak{p} \subset A$, there are $f \in A \setminus \mathfrak{p}$, elements $t_1, \ldots, t_n \in C$, and endomorphisms $\phi_1, \ldots, \phi_l \in H_f$, for some $l \leq n$, such that*

(1) C_f is a free A_f-module and $t_1, \ldots, t_n$ induce a basis for this module.

(2) H_f is a free C_f-module and $\phi_1, \ldots, \phi_l$ is a basis for this module.

(3) $\phi_i(t_j) = \delta_{ij}$ in C_f for $1 \leq i, j \leq l$.

Proof. We begin with some observations. As we noted in (1.22.1), there is an isomorphism of left C-modules:

$$\mathrm{End}_A(C) \simeq (C \otimes_A C)^* = \mathrm{Hom}_C(C \otimes_A C, C).$$

Since H is a C-direct summand of $\mathrm{End}_A(C)$, the inclusion of C-modules $H \subseteq \mathrm{End}_A(C)$ induces a surjective map $(\mathrm{End}_A(C))^* \to H^*$. Recall that any finitely generated and projective module is canonically isomorphic to its double dual (see Proposition 1.10). Thus, using the above identification for $\mathrm{End}_A(C)$, the dual map can be expressed as $C \otimes_A C \to P$ for some C-module P such that $H^* \simeq P$, and then $H \simeq H^{**} = \mathrm{Hom}_C(P, C)$. By Proposition 1.10, we deduce that P is finitely generated and projective as C-module. So from the surjection $C \otimes_A C \to P$, we conclude that P is a C-direct summand of $C \otimes_A C$.

Let $\mathfrak{p} \subset A$ be a prime ideal. By Proposition 1.7, $C_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of finite rank, say n. Thus, by Proposition A.38, we can choose $t_1, \ldots, t_n \in C$ that induce a basis for $C_{\mathfrak{p}}$ as $A_{\mathfrak{p}}$-module. Then the elements $1 \otimes t_1, \ldots, 1 \otimes t_n \in C \otimes_A C$ induce a basis for $C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} C_{\mathfrak{p}}$ as (left) $C_{\mathfrak{p}}$-module. Since the spectra are homeomorphic, $C_{\mathfrak{p}}$ is also a local ring. Recall that $P_{\mathfrak{p}}$ is a $C_{\mathfrak{p}}$-direct summand of $C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} C_{\mathfrak{p}}$. Thus, $P_{\mathfrak{p}}$ is also a free $C_{\mathfrak{p}}$-module of rank, say l. We can rearrange the terms if necessary, so the images of $1 \otimes t_1, \ldots, 1 \otimes t_l$ induce a basis for $P_{\mathfrak{p}}$ as $C_{\mathfrak{p}}$-module. Let $\phi_1, \ldots, \phi_l \in \mathrm{Hom}_{C_{\mathfrak{p}}}(P_{\mathfrak{p}}, C_{\mathfrak{p}})$ be the dual basis. By composition with $C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} C_{\mathfrak{p}} \to P_{\mathfrak{p}}$, we can consider the homomorphisms ϕ_i as elements of $\mathrm{Hom}_{C_{\mathfrak{p}}}(C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} C_{\mathfrak{p}}, C_{\mathfrak{p}})$. Then, if we identify each $1 \otimes t_j \in C \otimes_A C$ with its image in $C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} C_{\mathfrak{p}}$, we have $\phi_i(1 \otimes t_j) = \delta_{ij}$ in $C_{\mathfrak{p}}$ for all $1 \leq i, j \leq l$. Since localization $C \to C_{\mathfrak{p}}$ is flat and P is a finitely presented C-module, it follows by Lemma 1.24, that $H_{\mathfrak{p}} \simeq \mathrm{Hom}_{C_{\mathfrak{p}}}(P_{\mathfrak{p}}, C_{\mathfrak{p}})$. Therefore, we have proved that $t_1, \ldots, t_n \in C$ induce a basis for $C_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$ and that $\phi_1, \ldots, \phi_l$ is a basis for $H_{\mathfrak{p}}$ as $C_{\mathfrak{p}}$-module such that $\phi_i(t_j) = \delta_{ij}$.

Recall that the inclusion $A \subseteq C$ induces an homeomorphism between the spectra. Also, since C is finite and projective over A and H is finite and projective over C, we know by Proposition 1.7 that there exists $f \in A \setminus \mathfrak{p}$ such that $t_1, \ldots, t_n \in C$ induce a basis for C_f as A_f-module and $\phi_1, \ldots, \phi_l$ is a basis for H_f as C_f-module. Moreover, we can replace f by some product of f with another element, so we have also $\phi_i(t_j) = \delta_{ij}$ in C_f for all $1 \leq i, j \leq l$. □

Finally, the next proposition studies the ring of constants attached to certain unital subalgebras of the module endomorphisms of a finite projective extension of rings. The proof has several steps and its final part is inspired in the arguments given by S. Yuan in [67, Lemma 3.2], which are also based on G. Hochschild's proof of a slightly generalized form of the Jacobson-Bourbaki correspondence ([31, Theorem 2.1]). We make some modifications on these arguments to consider endomorphisms and finite projective extensions with homeomorphic spectra.

Proposition 1.28. *Let $A \subseteq C$ be a finite extension of rings such that C is projective as A-module. Assume in addition that the induced morphism $\operatorname{Spec}(C) \to \operatorname{Spec}(A)$ is an homeomorphism. Let $H \subseteq \operatorname{End}_A(C)$ be a unital A-subalgebra that is also a direct summand of $\operatorname{End}_A(C)$ as a C-submodule. Let $B_H := \{x \in C : [\varphi, x] = 0,\ \forall \varphi \in H\}$ be the ring of constants of H. Then $A \subseteq B_H \subseteq C$ is an intermediate subring and C is a finitely generated projective B_H-module. In addition, $H = \operatorname{End}_{B_H}(C)$.*

Proof. Recall that B_H is the subring of elements of C that are constants for every $\varphi \in H$, i.e., $x \in B_H$ if and only if $\varphi(xc) = x \cdot \varphi(c)$ for all $\varphi \in H$ and $c \in C$ (see discussion 1.22). It is clear that $A \subseteq B_H \subseteq C$ and, therefore $\operatorname{Spec}(B_H)$ is also homeomorphic to $\operatorname{Spec}(A)$ and $\operatorname{Spec}(C)$. By Proposition 1.7, the result follows if we prove that C is locally free of finite rank as B_H-module. Hence, we will prove that for each prime ideal $\mathfrak{p} \subset A$ there exists $f \in A \setminus \mathfrak{p}$ such that C_f is finitely generated and free as $(B_H)_f$-module.

We first show that B_H behaves well under localization. That is, we have to show that $S^{-1}B_H = B_{S^{-1}H}$ for any multiplicatively closed subset $S \subset A$. We consider the A-module $M := \operatorname{Hom}_A(H, \operatorname{End}_A(C))$. We define a map $\Phi\colon C \to M$ given by $\Phi(x) = [-, x]$ for any $x \in C$. Note that Φ is an homomorphism of A-modules whose kernel is B_H. Since H is C-module direct summand of $\operatorname{End}_A(C)$, which is a finite projective C-module, it follows by Proposition 1.2 that H is also a finite projective C-module. In addition, since C is a finite projective A-module, H is also a finite projective A-module by Proposition 1.5. In particular, H has finite presentation over A. Since localization $A \to S^{-1}A$, at any multiplicative subset $S \subset A$, is flat, we have by Lemma 1.24, an isomorphism of $S^{-1}A$-modules

$$S^{-1}M = S^{-1}\operatorname{Hom}_A(H, \operatorname{End}_A(C)) \simeq \operatorname{Hom}_{S^{-1}A}(S^{-1}H, \operatorname{End}_{S^{-1}A} S^{-1}C).$$

Since B_H is the kernel of Φ, we have that $S^{-1}B_H$ is the kernel of the map $S^{-1}C \to S^{-1}M$ induced by Φ when we localize. Using the above isomorphism, it is clear that $B_{S^{-1}H}$ coincides with the kernel of the induced map. Hence, we conclude that $S^{-1}B_H = B_{S^{-1}H}$.

By Lemma 1.27, we know that for each prime ideal $\mathfrak{p} \subset A$ there exists $f \in A \setminus \mathfrak{p}$, elements $t_1, \dots, t_n \in C$ and homomorphisms $\phi_1, \dots, \phi_n \in \operatorname{End}_{A_f}(C_f)$ such that $t_1, \dots, t_n$ induce a basis for C_f over A_f and $\phi_1, \dots, \phi_l$ is a basis for H_f as C_f-module such that $\phi_i(t_j) = \delta_{ij}$ for $1 \leq i, j \leq l$. In addition, we show that $\operatorname{Im}\phi_i \subseteq B_{H_f}$ for all $i = 1, \dots, l$. Since $\phi_1, \dots, \phi_l$ is a basis for H_f over C_f, any $\phi \in H_f$ can be expressed as $\phi = \sum_{k=1}^{l} \phi(t_k) \cdot \phi_k$. Recall that $C_f \subseteq H_f$ and that H_f is an A_f-algebra with the composition, so $\phi(x \cdot \phi_i) \in H_f$ for any $x \in C_f$. We have

$$\phi(x \cdot \phi_i) = \sum_{k=1}^{l} (\phi(x \cdot \phi_i))(t_k)\phi_k = \sum_{k=1}^{l} \phi(x \cdot \phi_i(t_k)) \cdot \phi_k = \phi(x) \cdot \phi_i.$$

In particular, if we evaluate the above expression on $c \in C_f$, we obtain $\phi(\phi_i(c) \cdot x) = \phi_i(c) \cdot \phi(x)$. Thus, for a fixed $c \in C_f$, we have

$$[\phi, \phi_i(c)](x) = \phi(\phi_i(c) \cdot x) - \phi_i(c) \cdot \phi(x) = 0, \qquad \text{for all } x \in C_f.$$

Therefore, $[\phi, \phi_i(c)] = 0$ for all $c \in C_f$ and $i = 1, \dots, l$. But this implies that $\phi_i(c) \in B_{H_f}$, as we wanted.

We prove now that $t_1, \dots, t_l$ form a basis for C_f over $(B_H)_f = B_{H_f}$. First, note that these elements are linearly independent over B_{H_f}. In fact, if $b_1 t_1 + \cdots + b_l t_l = 0$ for $b_i \in B_{H_f}$, after applying ϕ_i for $i = 1, \dots, l$, we get $b_1 = \cdots = b_l = 0$. It remains to show that $t_1, \dots, t_l$ generate C_f as B_{H_f}-module. Let $c \in C_f$ and define $c' := c - \sum_{j=1}^{l} \phi_j(c) t_j$. Using that $\phi_j(c) \in B_{H_f}$, we have $\phi_i(c') = \phi_i(c) - \phi_i(c) = 0$ for all $i = 1, \dots, l$. This implies that $\phi(c') = 0$ for all $\phi \in H_f$, as $\phi_1, \dots, \phi_l$ is a C_f-basis for H_f. Since H_f is a unital A_f-subalgebra, the identity endomorphism id_{C_f} is contained in H_f. Thus, we have $0 = \mathrm{id}_{C_f}(c') = c'$ and $c = \sum_{i=1}^{l} \phi_i(c) t_i$.

Finally, it is clear that any endomorphism in H is B_H-linear. Conversely, any $\phi \in \mathrm{End}_{B_H}(C)$ can be written locally as $\phi = \sum_{i=1}^{l} \phi(t_i) \cdot \phi_i$. Thus, $H = \mathrm{End}_{B_H}(C)$. □

Remark 1.29. Note that in the setting of Proposition 1.28, we have a tower of rings $A \subseteq B_H \subseteq C$ such that C is finite and projective as both an A-module and as a B_H-module. Thus, by Lemma 1.17, B_H is also finitely generated and projective as A-module.

The combination of Proposition 1.26 and Proposition 1.28 leads us to the next theorem that extends the Jacobson-Bourbaki correspondence for finite field extensions to a more general context of ring extensions.

Theorem 1.30. *Let $A \subseteq C$ be a finite extension of rings such that C is projective as A-module. In addition, assume that the induced morphism $\mathrm{Spec}(C) \to \mathrm{Spec}(A)$ is an homeomorphism. There is a bijection between the following subset of subrings*

$$\mathcal{P}_{C/A} := \left\{ B : \begin{array}{l} B \text{ is an intermediate subring } A \subseteq B \subseteq C \\ \text{and } C \text{ is a } B\text{-projective module} \end{array} \right\}$$

and the following subset of subalgebras

$$\mathcal{D}_{C/A} := \left\{ H : \begin{array}{l} H \text{ is an unital } A\text{-subalgebra of } \mathrm{End}_A(C) \text{ and} \\ \text{a direct summand of } \mathrm{End}_A(C) \text{ as } C\text{-module} \end{array} \right\}$$

given by the following inverse maps

$$\begin{array}{cccc} \mathcal{P}_{C/A} & \to \mathcal{D}_{C/A}, & \mathcal{D}_{C/A} & \to \mathcal{P}_{C/A} \\ B & \mapsto \mathrm{End}_B(C) & H & \mapsto B_H\,, \end{array}$$

where $B_H := \{x \in C : [\varphi, x] = 0,\ \forall \varphi \in H\}$. Moreover, for any subring $B \in \mathcal{P}_{C/A}$, B is finitely generated and projective as A-module and therefore $\mathrm{End}_A(B)$ is a finitely generated B-module.

As we show in the next example, Theorem 1.30 does not hold in general if $\mathrm{Spec}(A)$ and $\mathrm{Spec}(C)$ are not homeomorphic.

Example 1.31. Let K be a field and $L := K \times K$. We can view $K \subseteq L$ as a ring extension via the morphism $x \in K \mapsto (x, x) \in L$. We observe that $K \subset L$ is a

finite extension of rings such that L is projective as K-module. Indeed, L is a K-vector space of dimension 2. In addition, we note that the inclusion $K \subset L$ does not induce an homeomorphism between the spectra, since K has only one maximal ideal while L has two of them. Recall that $\mathrm{End}_K(L)$ can be identified with the matrices in $\mathbb{M}_{2\times 2}(K)$, where the structure as L-module is given by the left multiplication by diagonal matrices. Let H_1 and H_2 be the sets of upper and lower triangular matrices respectively. H_1 and H_2 are unital K-subalgebras of $\mathrm{End}_K(L)$ and also L-submodules that are direct summands of $\mathrm{End}_K(L)$. Moreover, the rings of constants attached to H_1 and H_2 are $B_{H_1} = B_{H_2} = K$. However, it is clear that $H_1 \neq H_2$, so the correspondence in Theorem 1.30 does not hold in this case.

1.4. Grassmannian of subalgebras

In this section, we revisit the concept of Grassmannian functor in order to parametrize certain intermediate subrings of a finite projective extension of rings with fixed rank. The original results from this section belong to [12, §4.2]

More precisely, let $A \subseteq C$ be a finite extension of rings such that C is a projective A-module of rank m. We want to parametrize the A-subalgebras B of C such that C is projective of a fixed rank over B. By Lemma 1.17, the rank of C over B is a positive integer q such that $q|m$ and the quotient C/B is also a projective A-module of rank $m - \frac{m}{q}$. The parametrization consists in defining a functor from the category of A-algebras to the category of sets which turns out to be representable by an A-scheme whose set of A-points is in bijection with the set of intermediate subrings B described before.

We begin with some preliminaries on the Grassmannian functor and its representability. We refer to [24, §8.4] and [26, I, §9.7] for a more detailed introduction.

1.32. *Grassmannian of submodules.* Let A be a ring and let M be an A-module. For any integer $n \geq 0$, we define the *Grassmannian functor of submodules* as

$$\begin{aligned} \mathrm{Grass}^n_{A,M} \colon \mathrm{Alg}_A &\to \mathrm{Sets} \\ A' &\mapsto \left\{ N' : \begin{array}{l} N' \text{ is an } A'\text{-submodule of } M' := M \otimes_A A', \\ M'/N' \text{ is a projective } A'\text{-module of rank } n \end{array} \right\} \end{aligned}$$

This functor is representable by an A-scheme ([26, I, Théorème 9.7.4]). This scheme is called the *Grassmannian* and it is denoted also by $\mathrm{Grass}^n_{A,M}$. Let $\pi \colon \mathrm{Grass}^n_{A,M} \to \mathrm{Spec}(A)$ be the structural morphism of $\mathrm{Grass}^n_{A,M}$ as an A-scheme and let $\mathscr{N} \subset \pi^* M$ be the universal bundle. The representability of $\mathrm{Grass}^n_{A,M}$ implies that for any A-algebra A', there is a natural bijection

$$\begin{aligned} \mathrm{Hom}_A(\mathrm{Spec}(A'), \mathrm{Grass}^n_{A,M}) &\simeq \mathrm{Grass}^n_{A,M}(A') \\ h &\mapsto h^* \mathscr{N} . \end{aligned} \tag{1.32.1}$$

Some geometric properties of the Grassmannian scheme are well-known. In fact, $\mathrm{Grass}^n_{A,M}$ is a projective A-scheme ([24, Proposition 8.14 and Proposition 8.17]). Moreover, if M is finitely generated (resp. of finite presentation) as A-module, then

$\mathrm{Grass}^n_{A,M}$ is an A-scheme of finite type (resp. of finite presentation) over A ([26, I, Proposition 9.7.7])

As we recall in the following proposition, the Grassmannian behaves-well under base change of rings.

Proposition 1.33 ([26, I, Proposition 9.7.6]). *Let A be a ring and let M be an A-module. For any integer $n \geq 0$ and any A-algebra A', there is an isomorphism of A'-schemes:*

$$\mathrm{Grass}^n_{A,M} \times_A \mathrm{Spec}(A') \simeq \mathrm{Grass}^n_{A',M\otimes_A A'}\,. \tag{1.33.1}$$

Now, we introduce the functor that parametrizes the subextensions of a finite projective ring extension of fixed rank, in which we are interested. We will show that this functor is representable as a subfunctor of the Grassmannian functor of modules.

1.34. *Grassmannian of subalgebras.* Let $A \subseteq C$ be a finite extension of rings such that C is projective of rank m as A-module. For any positive divisor $q|m$, we define the *Grassmannian functor of subalgebras* as the contravariant functor given by the association:

$$\begin{aligned}\mathcal{G}^q_{C/A}\colon \mathrm{Alg}_A &\to \mathrm{Sets}\\ A' &\mapsto \left\{B' : \begin{array}{l} B' \text{ is } A'\text{-subalgebra of } C' := C\otimes_A A',\\ C' \text{ is a projective } B'\text{-module of rank } q\end{array}\right\}\Bigg(\end{aligned}$$

In fact, for any $B' \in \mathcal{G}^q_{C/A}(A')$, it follows by Lemma 1.17 that the quotient C'/B' is a projective A' module of rank $m - \frac{m}{q}$. This shows that $\mathcal{G}^q_{C/A}$ is a subfunctor of the Grassmannian functor

$$\begin{aligned}\mathrm{Grass}^{m-\frac{m}{q}}_{A,C}\colon \mathrm{Alg}_A &\to \mathrm{Sets}\\ A' &\mapsto \left\{B' : \begin{array}{l} B' \text{ is an } A'\text{-submodule of } C' := C\otimes_A A',\\ C'/B' \text{ is a projective } A'\text{-module of rank } m-\frac{m}{q}\end{array}\right\},\end{aligned}$$

where we consider C with its structure as projective A-module of rank m.

Remark 1.35. Let $A \subseteq C$ be a finite extension of rings such that C is projective of rank m as A-module and let $A \to A'$ be any ring homomorphism. Recall from Remark 1.16 that $A' \subseteq C' := C \otimes_A A'$ is also a finite ring extension such that C' is projective over A' of the same rank. Therefore, by Proposition 1.33 and the nature of the definition of the functor $\mathcal{G}^q_{C/A}$, the inclusion of functors $\mathcal{G}^q_{C'/A'} \subseteq \mathrm{Grass}^{m-\frac{m}{q}}_{A',C'}$ is the base change of the inclusion $\mathcal{G}^q_{C/A} \subseteq \mathrm{Grass}^{m-\frac{m}{q}}_{A,C}$ by $A \to A'$.

Finally, we prove that this Grassmannian functor of subalgebras is representable. In each step of the proof we use [24, Proposition 8.4] which establishes some conditions for certain functors to be representable.

Theorem 1.36. *The Grassmannian functor of subalgebras $\mathcal{G}^q_{C/A}$ is representable by a quasi-projective A-scheme. More precisely, the inclusion of functors $\mathcal{G}^q_{C/A} \subseteq \mathrm{Grass}^{m-\frac{m}{q}}_{A,C}$ can be factorized as the composition of a quasi-compact open immersion followed by a closed immersion.*

Proof. By Lemma 1.20 and Remark 1.35, it is enough to prove the theorem under the assumption that A is Noetherian. We will express the inclusion $\mathcal{G}^q_{C/A} \subseteq \mathrm{Grass}^{m-\frac{m}{q}}_{A,C}$ as a composition

$$\mathcal{G}^q_{C/A} \to \mathcal{G}_2 \to \mathcal{G}_1 \to \mathrm{Grass}^{m-\frac{m}{q}}_{A,C}$$

where $\mathcal{G}_1 \to \mathrm{Grass}^{m-\frac{m}{q}}_{A,C}$ and $\mathcal{G}_2 \to \mathcal{G}_1$ will be closed immersions and $\mathcal{G}^q_{C/A} \to \mathcal{G}_2$ will be an open immersion, which is necessarily quasi-compact since A is a Noetherian ring (see [24, Lemma 1.5]). First, we define the functors $\mathcal{G}_1$ and $\mathcal{G}_2$.

Let A' be any A-algebra and set $C' := C \otimes_A A'$. Then $A' \subseteq C'$ is also a finite extension such that C' is a projective A'-module of rank m (see Remark 1.16). For any A'-submodule $B' \subseteq C$, we have that $B' \in \mathcal{G}^q_{C/A}(A')$ if and only if $B' \in \mathrm{Grass}^{m-\frac{m}{q}}_{A,C}(A')$ and it is is also an A'-subalgebra of C' such that C' is projective of rank q as B'-module. Hence, we define the functor

$$\begin{aligned}\mathcal{G}_1\colon\ &\mathrm{Alg}_A \to \mathrm{Sets}\\ &A' \mapsto \left\{B' \in \mathrm{Grass}^{m-\frac{m}{q}}_{A,C}(A') : B' \text{ is an } A'\text{-subalgebra of } C'\right\}\Bigg(\end{aligned}$$

so $B' \in \mathcal{G}^q_{C/A}(A')$ if and only if $B' \in \mathcal{G}_1(A')$ and C' is projective of rank q as B'-module. Since C' is finite over A', it follows that C' is also finite over any A'-submodule B'. Therefore by Proposition 1.14 we have that C' is a projective B'-module of rank q if and only if $\mathrm{Fitt}^{B'}_{q-1}(C') = 0$ and $\mathrm{Fitt}^{B'}_q(C') = B'$. Thus, we define the functor

$$\begin{aligned}\mathcal{G}_2\colon\ &\mathrm{Alg}_A \to \mathrm{Sets}\\ &A' \mapsto \{B' \in \mathcal{G}_1(A') : \mathrm{Fitt}^{B'}_{q-1}(C') = 0\},\end{aligned}$$

so $B' \in \mathcal{G}^q_{C/A}(A')$ if and only if $B' \in \mathcal{G}_2(A')$ and $\mathrm{Fitt}^{B'}_q(C') = B'$. So we can describe $\mathcal{G}^q_{C/A}$ as the subfunctor of $\mathcal{G}_2$ given by

$$\begin{aligned}\mathcal{G}^q_{C/A}\colon\ &\mathrm{Alg}_A \to \mathrm{Sets}\\ &A' \mapsto \{B' \in \mathcal{G}_2(A') : \mathrm{Fitt}^{B'}_q(C \otimes_A A') = B'\}.\end{aligned}$$

Now, we prove that the inclusion $\mathcal{G}_1 \subseteq \mathrm{Grass}^{m-\frac{m}{q}}_{A,C}$ is a closed immersion. Let $\pi\colon \mathrm{Grass}^{m-\frac{m}{q}}_{A,C} \to \mathrm{Spec}(A)$ be the structural morphism and let $\mathscr{B} \subset \pi^*C$ be the universal bundle. So for any A-algebra A', we have a natural bijection

$$\begin{aligned}\mathrm{Hom}_A(\mathrm{Spec}(A'), \mathrm{Grass}^{m-\frac{m}{q}}_{A,C}) &\simeq \mathrm{Grass}^{m-\frac{m}{q}}_{A,C}(A')\\ h &\mapsto h^*\mathscr{B}.\end{aligned} \tag{1.36.1}$$

We consider the following compositions of natural morphisms of sheaves on $\mathrm{Grass}^{m-\frac{m}{q}}_{A,C}$:

$$\begin{aligned}v\colon \mathscr{B} \otimes \mathscr{B} \to \pi^*C \otimes \pi^*C \to \pi^*C \to \pi^*C/\mathscr{B},\\ w\colon \pi^*A \to \pi^*C \to \pi^*C/\mathscr{B},\end{aligned}$$

where the middle morphism in the definition of v is induced by the multiplication of the A-algebra C. Given an A-algebra A' and $h \in \mathrm{Hom}_A(\mathrm{Spec}(A'), \mathrm{Grass}_{A,C}^{m-\frac{m}{q}})$, the condition $h^*v = 0$ asserts that the A'-submodule $h^*\mathscr{B} \subseteq C \otimes_A A'$ is closed under the multiplication of C', and the condition $h^*w = 0$ asserts that $A' \subseteq h^*\mathscr{B}$. Thus, having $h^*v = 0$ and $h^*w = 0$ is equivalent to $h^*\mathscr{B} \in \mathcal{G}_1(A')$. Since $\pi^*C/\mathscr{B}$ is finite locally free, $\mathcal{G}_1$ is representable and the inclusion $\mathcal{G}_1 \subseteq \mathrm{Grass}_{A,C}^{m-\frac{m}{q}}$ is a closed immersion, by [24, Proposition 8.4].

We prove now that the inclusion $\mathcal{G}_2 \subseteq \mathcal{G}_1$ is a closed immersion. Let $\pi\colon \mathcal{G}_1 \to \mathrm{Spec}(A)$ be the structural morphism and let $\mathscr{B}_1 \subseteq \pi^*C$ be the universal subalgebra. So for any A-algebra A', we have a natural bijection

$$\begin{aligned} \mathrm{Hom}_A(\mathrm{Spec}(A'), \mathcal{G}_1) &\simeq \mathcal{G}_1(A') \\ h &\mapsto h^*\mathscr{B}_1\,. \end{aligned} \tag{1.36.2}$$

Let $v_{q-1}\colon \mathrm{Fitt}_q^{\mathscr{B}_1}(\pi^*C) \to \mathscr{B}_1$ denote the inclusion of the $(q-1)$-th Fitting ideal of the $\mathscr{B}_1$-module π^*C. Given an A-algebra A' and a morphism of A-schemes $h\colon \mathrm{Spec}(A') \to \mathcal{G}_1$, the Fitting ideal $\mathrm{Fitt}_{q-1}^{h^*\mathscr{B}_1}(C')$ is the image of the pullback h^*v_{q-1}, by the good behaviour of the Fitting ideals under base change (see 1.13). Hence, under the bijection (1.36.2), the inclusion $\mathcal{G}_2(A') \subseteq \mathcal{G}_1(A')$ corresponds to those A-morphisms h such that $h^*v_{q-1} = 0$. Since $\mathscr{B}_1$ is finite locally free, $\mathcal{G}_2$ is representable and the inclusion $\mathcal{G}_2 \subseteq \mathcal{G}_1$ is a closed immersion, by [24, Proposition 8.4].

Finally, we prove that the inclusion $\mathcal{G}_{C/A}^q \subseteq \mathcal{G}_2$ is an open immersion. Let $\pi\colon \mathcal{G}_2 \to \mathrm{Spec}(A)$ be the structural morphism and let $\mathscr{B}_2 \subseteq \pi^*C$ be the universal bundle. So for any A-algebra A', we have a natural bijection

$$\begin{aligned} \mathrm{Hom}_A(\mathrm{Spec}(A'), \mathcal{G}_2) &\simeq \mathcal{G}_2(A') \\ h &\mapsto h^*\mathscr{B}_2\,. \end{aligned} \tag{1.36.3}$$

Consider now the map $v_q\colon \mathrm{Fitt}_q^{\mathscr{B}_2}(\pi^*C) \to \mathscr{B}_2$. By the same token as in the proof that $\mathcal{G}_2 \subseteq \mathcal{G}_1$ is a closed immersion, one can show that, under the natural bijection (1.36.3), the inclusion $\mathcal{G}_{C/A}^q(A') \subseteq \mathcal{G}_2(A')$ is in correspondence with those A-morphisms $h\colon \mathrm{Spec}(A') \to \mathcal{G}_2$ such that h^*v_q is surjective. We conclude by [24, Proposition 8.4] that the inclusion $\mathcal{G}_{C/A}^q \hookrightarrow \mathcal{G}_2$ is an open immersion. This completes the proof of the theorem. □

CHAPTER 2

Purely inseparable Galois extensions of exponent one

This chapter is dedicated to the study of *purely inseparable extensions of exponent at most one*, that is, commutative ring extensions with unity $A \subseteq C$ of prime characteristic $p > 0$ such that

(i) $C^p \subseteq A$;

(ii) C is a finitely generated and projective A-module; and

(iii) for each prime ideal $\mathfrak{p} \subset A$, there is a faithfully flat extension $A_\mathfrak{p} \to A'$ such that $C_\mathfrak{p} \otimes_{A_\mathfrak{p}} A'$ is isomorphic to an A'-algebra of the form $A'[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$ for some $n \geq 0$.

These extensions are also called *Galois extensions of exponent one* and belong to the class of finite projective extensions of rings that we studied in the previous chapter. They were introduced by S. Yuan in [68], where he extended the Jacobson's Galois theory of purely inseparable field extensions of exponent one ([35], [36]) to the setting of rings. This is why he called these extensions purely inseparable Galois, or simply Galois. We warn the reader that this notion differs from the classical notion of Galois extensions usually defined for separable field extensions.

Throughout this chapter, we show that Galois extensions of rings admit many characterizations, some of them consist of replacing condition (iii) of the above definition. In fact, the original definition of Galois extension substitutes condition (iii) in our definition of purely inseparable extension of exponent one by the next property:

(iv) C has locally, at each prime ideal, a p-basis over A.

Furthermore, S. Yuan's results from [66] and [68] show that Galois extensions are related to the notions of differentiably simple rings and derivations. Indeed, they show that for a finite projective extension of exponent at most one to be Galois, the conditions (iv), which define purely inseparable ring extensions of exponent at most one, can be replaced by each of the following properties:

(v) for each prime ideal $\mathfrak{p} \subset A$, the ring $C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ is differentiably simple.

(vi) $\mathrm{End}_A(C) = C[\mathrm{Der}_A(C)]$ as A-algebras.

Our first interest is to enlarge the list of conditions that characterize Galois extensions, with a view to extending the study to purely inseparable extensions of higher exponent later on in Chapter 3. On the one hand, we note that the connection between derivations and Galois extensions is broader. By considering the derivations as a submodule of the module of endomorphisms of the extension, we show that condition (iv) can be replaced also by the next property:

(vii) $\mathrm{Der}_A(C)$ is a C-module direct summand of $\mathrm{End}_A(C)$.

On the other hand, we recover the well-known relation between p-basis and the module of differentials studied by E. Kunz in [44, §5]. Using this connection, it can be shown that Galois extensions are finite ring extensions of exponent at most one such that the module of differentials $\Omega_{C/A}$ is a projective C-module.

S. Yuan's motivation to study Galois extensions was to develop a Galois theory for purely inseparable ring extensions of exponent one. With this aim, he studied the intermediate subrings B of a Galois extension $A \subseteq C$ such that $B \subseteq C$ and, hence, $A \subseteq B$ are also Galois. We will refer to a tower of rings $A \subseteq B \subseteq C$ satisfying these conditions as a *Galois tower of rings*. Moreover, given $A \subseteq C$ a Galois extension and B an intermediate subring, M. André ([1]) proved using homological methods that $A \subseteq B \subseteq C$ is a Galois tower if and only if C is projective as a B-module.

Our second interest has to do with Galois towers of rings. Given a Galois extension $A \subseteq C$ of constant rank, we parametrize the intermediate subrings B of fixed rank such that $A \subseteq B \subseteq C$ is a Galois tower by a Grassmannian functor of subalgebras as in the first chapter. This functor is in fact an A-scheme, which we call *Yuan scheme*, so we analyse some of its geometric properties.

Organization. This chapter is divided into three sections. The first one contains various preliminaries needed to study Galois extensions of rings. A large part of the section is expository and revisits some well-known results that can be found in [12, §2 and §3], [44, §5 and §15], [66] and [68]. The second section is devoted to Galois extensions of exponent one and its different characterizations, while the third section addresses towers of Galois extensions. Both last sections include a review of the results from S. Yuan ([68]) and new results from [12] and [11] that complete the understanding of Galois extensions and towers respectively. Those new results are joint work from the author of this thesis and D. Sulca, and also partially from the collaboration with O. Villamayor.

Section 2.1 collects some preliminaries on derivations, modules of Kähler differentials, p-basis and differentiably simple rings. We emphasize on the relation between these notions to understand later Galois extensions. In particular, we give alternative proofs for some important results on differentiably simple rings (Theorem 2.33 and Theorem 2.39).

Section 2.2 includes the main properties of Galois extensions and their characterizations in terms of differentiably simple rings, modules of differentials and modules of derivations (Theorem 2.71).

Section 2.3 focuses on Galois towers of rings. We introduce a parametrization for the subrings of a Galois extension that induce a Galois tower of fixed differential ranks (Definition 2.87). More precisely, given a Galois extension $A \subseteq C$ of fixed differential rank n and an integer $0 \leq r \leq n$, we study the intermediate subrings $A \subseteq B \subseteq C$ such that $B \subseteq C$ is a Galois extension of differential rank r, and so $A \subseteq B$ is also Galois of differential rank $n-r$. We define the *Yuan functor* from the category of sets on the category of A-algebras, whose set of A-points is formed by the tower of rings described before. We show that this functor is representable by a quasi-projective A-scheme (Theorem 2.92) and we study some of its geometric properties (Theorem 2.95).

2.1. Preliminaries for Galois extensions

This section contains basic concepts and results which are necessary to study Galois extensions of rings, defined as in the previous introduction. In Subsection 2.1.1, we revise the notion of exponent of a ring extension and some basic properties. In Subsection 2.1.2, we introduce derivations and Kähler differentials. In Subsection 2.1.3, we include a quick overview on p-basis. Finally, Subsection 2.1.4 is devoted to differentiably simple rings, in particular, we give alternative proofs for some important results. Throughout, p denotes a fixed rational prime.

2.1.1. Exponent of a ring extension

In this subsection, all the rings are assumed to have prime characteristic p. We begin with the notion of exponent for a ring extension.

Definition 2.1. Let $A \subseteq C$ be a ring extension. An element $x \in C$ has *finite exponent* over A if there exists an integer $e \geq 0$ such that $x^{p^e} \in A$. The extension $A \subseteq C$ has *finite exponent* if there is an integer e such that every $x \in C$ has exponent at most e. The minimal e with this property is the *exponent* of the extension and we denote it by $\exp(C/A)$. Note that for a trivial extension $A = C$ the exponent is zero, and the converse is also true.

Remark 2.2. If $A \subseteq C$ is a ring extension with finite exponent $\exp(C/A) = e$. Then $\operatorname{Spec}(A)$ and $\operatorname{Spec}(C)$ are canonically homeomorphic, since the ring maps

$$\begin{aligned} A \to C; \quad C \to A, \\ x \mapsto x; \quad x \mapsto x^{p^e}. \end{aligned}$$

induce continuous and mutually inverse maps on the spectra. Thus, any prime ideal $\mathfrak{P} \subset C$ can be identified with a unique prime ideal $\mathfrak{p} \subset A$ and any open covering for $\operatorname{Spec}(A)$ induces an open covering for $\operatorname{Spec}(C)$ and vice versa.

The following lemma shows that the identification of the prime ideals from the previous remark induce a natural identification for the modules obtained by localization at prime ideals. The proof of the lemma uses the same argument as the proof of [68, Lemma 3], which was stated only for ring extensions of exponent at most one.

Lemma 2.3. *Let $A \subseteq C$ be a ring extension with finite exponent. Let $\mathfrak{P} \subset C$ be a prime ideal and let $\mathfrak{p} \subset A$ be the corresponding prime ideal via the induced homeomorphism $\mathrm{Spec}(C) \to \mathrm{Spec}(A)$ from Remark 2.2. For any C-module M, there is a natural identification $M_{\mathfrak{P}} = M \otimes_A A_{\mathfrak{p}} =: M_{\mathfrak{p}}$.*

Proof. Let $e := \exp(C/A)$. We have a natural homomorphism

$$C \otimes_A A_{\mathfrak{p}} \to C_{\mathfrak{P}}, \quad x \otimes \frac{a}{s} \mapsto \frac{ax}{s} \qquad \text{for } x \in C,\ a \in A \text{ and } s \in A \setminus \mathfrak{p}.$$

This map is surjective, since $(x/t) \in C_{\mathfrak{P}}$, with $t \in C \setminus \mathfrak{P}$, is the image of the element $(xt^{p^e-1}) \otimes (1/t^{p^e}) \in C \otimes_A A_{\mathfrak{p}}$. We claim that the map is injective. Note that any element in $C \otimes_A A_{\mathfrak{p}}$ can be written as

$$\sum_i x_i \otimes \frac{a_i}{s_i} = x \otimes \frac{1}{s}, \quad \text{where } x = \sum_i a_i x_i \cdot \Big(\prod_{æ \neq i} s_j\Big) \text{ and } s = \prod_i s_i.$$

If $x \otimes (1/s) \mapsto (x/s) = 0 \in C_{\mathfrak{P}}$, then there is $t \in C \setminus \mathfrak{P}$ such that $tx = 0 \in C$. Thus, we have

$$x \otimes \frac{1}{s} = (t^{p^e} x) \otimes \frac{1}{t^{p^e} s} = 0 \in C \otimes_A A_p.$$

Therefore, we have $C \otimes_A A_{\mathfrak{p}} = C_{\mathfrak{P}}$. Then for any C-module M, we conclude that

$$M_{\mathfrak{P}} = M \otimes_C C_{\mathfrak{P}} = M \otimes_C C \otimes_A A_{\mathfrak{p}} = M \otimes_A A_{\mathfrak{p}}.$$

□

We introduce some notation for intermediate subalgebras that are of interest in the study of the exponent of a ring extension. These intermediate subalgebras will be of great interest and use later on in Chapter 3, when we study purely inseparable extensions of rings.

2.4. *Some intermediate subalgebras.* Let C be an A-algebra. For each integer $e \geq 0$, we denote by

$$C^{[e]} := A[C^{p^e}],$$

the A-subalgebra of C generated by all elements of the form x^{p^e} with $x \in C$. Since C can be considered as an A-module, $C^{[e]}$ is also an A-submodule of C. Note that if C is a finitely generated A-algebra, then so is each subalgebra $C^{[e]}$. In addition, if $A \subseteq C$ is a ring extension of finite exponent, we have $C^{[e]} = A$ for all $e \geq \exp(C/A)$ and, therefore, there is a tower of ring extensions

$$A \subset C^{[\exp(C/A)-1]} \subset \ldots \subset C^{[2]} \subset C^{[1]} \subset C,$$

where each subextension $C^{[e+1]} \subset C^{[e]}$ has exponent one for $0 \leq e < \exp(C/A)$.

Remark 2.5. Let $A \subseteq C$ be a ring extension and let $e \geq 0$ be any integer. Note that $C^{p^e} \subseteq A$ as subrings of C if and only if $C^{[e]} := A[C^{p^e}] = A$ as A-submodules of C. Let $\pi\colon C \to C/A$ be the quotient homomorphism of A-modules. Then $C^{[e]} = A$ if and only if $\pi(C^{[e]}) = 0$. Therefore, $A \subseteq C$ has exponent e if and only if e is the minimal integer such that $\pi(C^{[e]}) = 0$.

The next lemma shows that, under certain flatness hypothesis, the submodules induced by the subalgebras in the previous discussion behave well under base extensions.

Lemma 2.6. *Let $A \subseteq C$ be a finite ring extension and let A' be an A-algebra. Assume that either $A \to A'$ is flat; or $C^{[e+1]} \to C^{[e]}$ is flat for all $e \geq 0$. Then $(C \otimes_A A')^{[e]} = C^{[e]} \otimes_A A'$ as A'-submodules of $C \otimes_A A'$ for all $e \geq 0$.*

Proof. We first prove that $C^{[e]} \otimes_A A'$ is an A'-subalgebra of $C \otimes_A A'$. On the one hand, if $A \to A'$ is flat, it is clear that the base change of $C^{[e]} \subseteq C$ induces an inclusion $C^{[e]} \otimes_A A' \subseteq C \otimes_A A'$ for all $e \geq 0$. On the other hand, we assume that $C^{[e+1]} \to C^{[e]}$ is flat for all $e \geq 0$. Since $C^{[e+1]} \subseteq C^{[e]}$ has exponent one, the spectra are homeomorphic (see Remark 2.2). In particular, the induced map on the spectra, $\operatorname{Spec}(C^{[e+1]}) \to \operatorname{Spec}(C^{[e]})$, is surjective. Then $C^{[e+1]} \to C^{[e]}$ is faithfully flat by Proposition A.19. Moreover, $C^{[e+1]} \otimes_A A' \to C^{[e]} \otimes_A A'$ is also faithfully flat by Proposition A.16. In particular, the map is injective, so $C^{[e+1]} \otimes_A A' \subseteq C^{[e]} \otimes_A A'$. Since $C^{[0]} \otimes_A A' = C \otimes_A A'$ and, we conclude that $C^{[e]} \otimes_A A' \subseteq C \otimes_A A'$ as A'-modules for all $e \geq 0$.

We show that, in both cases, the subring $C^{[e]} \otimes_A A'$ coincides with $(C \otimes_A A')^{[e]}$ for all $e \geq 0$. Since $A \subseteq C$ is finite, we can write $C = A[x_1, \ldots, x_n]$ for some $x_1, \ldots, x_n \in C$ and then $C^{[e]} = A[x_1^{p^e}, \ldots, x_n^{p^e}]$ for all $e \geq 0$. Hence, we have $C \otimes_A A' = A'[y_1, \ldots, y_n]$ where $y_i := x_i \otimes 1$. Note that $y_i^{p^e} = (x_i \otimes 1)^{p^e} = x_i^{p^e} \otimes 1$. Thus, we conclude that $C^{[e]} \otimes_A A' = A'[y_1^{p^e}, \ldots, y_n^{p^e}] = (C \otimes_A A')^{[e]}$, as we wanted. □

Remark 2.7. The proposition above applies in particular for $A' = A_{\mathfrak{p}}$ where $\mathfrak{p} \subset A$ is any prime ideal. Since localization $A \to A_{\mathfrak{p}}$ is flat, we have that $(C_{\mathfrak{p}})^{[e]} = (C^{[e]})_{\mathfrak{p}}$. Thus, we can just write $C_{\mathfrak{p}}^{[e]}$ without confusion.

Using the above results we deduce some properties of the exponent for some ring extensions. The next lemma studies the behaviour of the exponent of certain finite ring extensions under base change. It applies for instance for finite projective ring extensions or for base change via flat homomorphisms as localization.

Lemma 2.8. *Let $A \subseteq C$ be a finite ring extension of finite exponent and let A' be an A-algebra. Denote $C' := C \otimes_A A'$. Assume that either $A \to A'$ is flat; or $C^{[e+1]} \to C^{[e]}$ is flat for all $e \geq 0$. Then $A' \subseteq C'$ has finite exponent and* $\exp(C'/A') \leq \exp(C/A)$.

Proof. We note that, under these hypothesis, we have $C'^{[e]} = C^{[e]} \otimes_A A' \subseteq C'$ for all $e \geq 0$ by Lemma 2.6. Since $A \subseteq C$ has finite exponent, we have $C^{[e]} = A$ for $e \geq \exp(C/A)$ and so $C'^{[e]} = A'$. Thus, we have $A' \subseteq C'$.

We claim that $C'/A' = C/A \otimes_A A'$. In fact, the short exact sequence of A-modules $0 \to A \to C \to C/A \to 0$ induces a right exact sequence

$$A' \to C \otimes_A A' \to (C/A) \otimes_A A' \to 0.$$

If $A \to A'$ is flat, then the above sequence is also left exact. If $C^{[e+1]} \to C^{[e]}$ is flat, then it is faithfully flat as shown in the proof of Lemma 2.6. Since $A \subseteq C$ has finite exponent, it follows from Proposition A.17 that $A \to C$ is faithfully flat. Then C/A is also flat (Proposition A.18) and the above exact sequence is also left exact. Hence, we have proved that $0 \to A' \to C' \to (C/A) \otimes_A A' \to 0$ in both cases, and this implies that $C'/A' = (C/A) \otimes_A A'$, as we wanted.

Let $\pi\colon C \to C/A$ and $\pi'\colon C' \to C'/A'$ be the quotient maps. If $\exp(C/A) = e$, then $\pi(C^{[e]}) = 0$ as we noted in Remark 2.5. Thus, using that $C'/A' = (C/A) \otimes_A A'$ and $C'^{[e]} = C^{[e]} \otimes_A A'$, we have

$$0 = \pi(C^{[e]}) \otimes_A A' = \pi'(C^{[e]} \otimes_A A') = \pi(C'^{[e]}).$$

Therefore, we conclude that $A' \subseteq C'$ has finite exponent and that $\exp(C'/A') \leq e$ by Remark 2.5. □

Moreover, we show that the exponent of a finite ring extension is descents by faithfully flat base change.

Lemma 2.9. *Let $A \subseteq C$ be a finite ring extension. Let $A \to A'$ be a faithfully flat homomorphism of rings. Denote $C' := C \otimes_A A'$. If $A' \subseteq C'$ has finite exponent, then $A \subseteq C$ has finite exponent and* $\exp(C/A) = \exp(C'/A')$.

Proof. Since $A \to A'$ is faithfully flat, we have $A' \subseteq C'$ and $C'/A' = (C/A) \otimes_A A'$. In addition, we can apply Lemma 2.6 so $C'^{[e]} = C^{[e]} \otimes_A A' \subseteq C'$ for all $e \geq 0$. Let $\pi\colon C \to C/A$ and $\pi'\colon C' \to C'/A'$ be the quotient maps. Then we have

$$\pi(C'^{[e]}) = \pi'(C^{[e]} \otimes_A A') = \pi(C^{[e]}) \otimes_A A'.$$

Since $A \to A'$ is faithfully flat, $\pi(C'^{[e]}) = 0$ if and only if $\pi(C^{[e]}) = 0$. By Remark 2.5, we know that e is the minimum integer such that $\pi(C'^{[e]}) = 0$, and also the minimum such that $\pi(C^{[e]}) = 0$. Hence, we conclude that $A \subseteq C$ has finite exponent and $\exp(C/A) = e = \exp(C'/A')$. □

Finally, we demonstrate in the next lemma that the exponent of a finite ring extension can be determined by the exponent of the ring extensions obtained by localization at prime ideals.

Lemma 2.10. *Let $A \subseteq C$ be a finite ring extension and let $e \geq 0$ be an integer. Then $A \subseteq C$ has finite exponent* $\exp(C/A) = e$ *if and only if* $\max\{\exp(C_\mathfrak{p}/A_\mathfrak{p}) : \mathfrak{p} \in \operatorname{Spec}(A)\}$ *exists and is equal to e.*

Proof. Since localization $A \to A_\mathfrak{p}$ is flat, we have an inclusion $A_\mathfrak{p} \subseteq C_\mathfrak{p} = C \otimes_A A_\mathfrak{p}$ for each prime $\mathfrak{p} \subset A$. Let $\pi\colon C \to C/A$ and $\pi_\mathfrak{p}\colon C_\mathfrak{p} \to C_\mathfrak{p}/A_\mathfrak{p}$ be the quotient maps.

By Lemma A.9 and Remark 2.7, we have $\pi(C^{[e]}) = 0$ if and only if $\pi_{\mathfrak{p}}(C_{\mathfrak{p}}^{[e]}) = 0$ for every prime ideal $\mathfrak{p} \subset A$. Since the exponent of an extension is the minimum e with this property (Remark 2.5), we conclude that $\exp(C/A) = e$ if and only if $\max\{\exp(C_{\mathfrak{p}}/A_{\mathfrak{p}}) : \mathfrak{p} \in \operatorname{Spec}(A)\} = e$. □

2.1.2. Derivations and Kähler differentials

We return in this subsection to the general setting of rings of any characteristic, commutative with unity. We give a brief introduction on derivations and review the construction of the module of Kähler differentials and the universal derivation. We mostly follow the approach from E. Kunz in [44].

2.11. *Module of derivations.* Let C be an A-algebra and let M be a C-module. An homomorphism of A-modules $D\colon C \to M$ is an *A-derivation from C to M* that satisfies the Leibniz rule

$$D(c_1c_2) = c_1D(c_2) + c_2D(c_1) \quad \text{for all } c_1, c_2 \in C.$$

We denote by $\operatorname{Der}_A(C, M)$ the set of A-derivations, which is also a C-submodule of $\operatorname{Hom}_A(C, M)$. Observe that the construction of $\operatorname{Der}_A(C, M)$ is functorial in M.

2.12. *Module of Kähler differentials.* We consider now the A-algebra $C \otimes_A C$, which has an structure as both left and right C-module. Let J be the kernel of the multiplication map

$$C \otimes_A C \to C, \quad c_1 \otimes c_2 \mapsto c_1 \cdot c_2.$$

Note that J is generated as a C-module by the elements of the form $1 \otimes c - c \otimes 1$ with $c \in C$. We set $\Omega_{C/A} := J/J^2$ and consider it with the structure of C-module induced from the structure of left C-module in $C \otimes_A C$. The C-module $\Omega_{C/A}$ is the module of *Kähler differentials* and the *universal A-derivation* is given by the map $d\colon C \to \Omega_{C/A}$ which associates to each $c \in C$ the class of $1 \otimes c - c \otimes 1$ ([44, Definition 1.20]). We note that d is an A-derivation satisfying the following universal property:

Proposition 2.13 ([44, Proposition 1.23])**.** *Let C be an A-algebra and let M be a C-module. Then for any A-derivation $D\colon C \to M$ there is only one C-linear map $\varphi\colon \Omega_{C/A} \to C$ such that $D = \varphi \circ d$. Equivalently, there is an isomorphism of C-modules*

$$\operatorname{Hom}_C(\Omega_{C/A}, M) \xrightarrow{\sim} \operatorname{Der}_A(C, M), \quad \varphi \mapsto \varphi \circ d.$$

We recall the two fundamental exact sequences of the modules of Kähler differentials.

Proposition 2.14 (First fundamental exact sequence, [44, Proposition 3.24])**.** *Let $B \to C$ be an homomorphism of A-algebras. Then there is an exact sequence of C-modules*

$$C \otimes_B \Omega_{B/A} \to \Omega_{C/A} \to \Omega_{C/B} \to 0.$$

Proposition 2.15 (Second fundamental exact sequence, [44, Proposition 4.17]). *Let $\varphi\colon B \to C$ be a surjective homomorphism of A-algebras. Let : $I = \ker(\varphi)$, so $C \simeq B/I$. Then there is an exact sequence of C-modules*

$$I/I^2 \to C \otimes_B \Omega_{B/A} \to \Omega_{C/A} \to 0.$$

The following proposition shows that finiteness conditions for C as an A-algebra induce good finiteness properties in $\Omega_{C/A}$ as C-module.

Proposition 2.16. *Let C be an A-algebra.*

(1) If C is a finitely generated A-algebra, then $\Omega_{C/A}$ is finitely generated as C-module.

(2) If C has finite presentation as an A-algebra, then $\Omega_{C/A}$ has finite presentation as C-module.

Proof. Let $d\colon C \to \Omega_{C/A}$ be the universal A-derivation. As it is noted in [44, Remark 1.20], the C-module $\Omega_{C/A}$ is generated by $\{dc : c \in C\}$. First, we assume that C is a finitely generated A-algebra, say $C = A[x_1, \ldots, x_n]$. By an application of the Leibniz rule, it is clear that $dx_1, \ldots, dx_n$ generate $\Omega_{C/A}$ as C-module. Hence, we have proved (1).

Now, we assume that C has finite presentation as A-algebra, so $C = A[X_1, \ldots, X_n]/I$ for some finitely generated ideal I. Set $B := A[X_1, \ldots, X_n]$. Then by Proposition 2.15, the second fundamental exact sequence reads as

$$I/I^2 \to C \otimes_B \Omega_{B/A} \to \Omega_{C/A} \to 0.$$

Note that I/I^2 is finitely generated, since so is I. Let N be the kernel of the surjective homomorphism $C \otimes_B \Omega_{B/A} \to \Omega_{C/A}$. Since N is the image of I/I^2 in $C \otimes_B \Omega_{B/A}$ via the map in the above exact sequence, we deduce that N is also finitely generated. Observe also that $C \otimes_B \Omega_{B/A}$ is free (see [44, Example 2.5.(d)]). Thus, applying Proposition A.25.(4) to the short exact sequence $0 \to N \to C \otimes_B \Omega_{B/A} \to \Omega_{C/A} \to 0$, we conclude that $\Omega_{C/A}$ has finite presentation as C-module. □

The modules of differentials behave well also under base change. In particular, these modules have a good behaviour under localization, and the same occurs with the modules of derivations under some finiteness conditions.

Proposition 2.17 ([44, Proposition 4.21 and Corollary 4.22]). *Let C be an A-algebra and let $A \to A'$ be any homomorphism of rings. Let $C' := C \otimes_A A'$. Then there is a natural isomorphism*

$$\Omega_{C'/A'} \simeq \Omega_{C/A} \otimes_C C'.$$

In particular, if $S \subseteq A$ any multiplicative subset, there is a natural isomorphism $\Omega_{S^{-1}C/S^{-1}A} \simeq S^{-1}\Omega_{C/A}$.

Corollary 2.18. *Let C be an A-algebra of finite presentation and let M be any C-module. For every multiplicatively closed subset $S \subseteq A$, there is natural isomorphism*

$$S^{-1}\operatorname{Der}_A(C,M) \xrightarrow{\sim} \operatorname{Der}_{S^{-1}A}(S^{-1}C, S^{-1}M).$$

Proof. By Proposition 2.13, we have $S^{-1}\operatorname{Der}_A(C,M) \simeq S^{-1}\operatorname{Hom}_C(\Omega_{C/A}, M)$. By Proposition 2.16, the C-module $\Omega_{C/A}$ has finite presentation. Since localization is flat, we can apply Lemma 1.24 to obtain an isomorphism $S^{-1}\operatorname{Hom}_C(\Omega_{C/A}, M) \simeq \operatorname{Hom}_{S^{-1}C}(\Omega_{S^{-1}C/S^{-1}A}, S^{-1}M)$. Finally, by Proposition 2.13, we have

$$\operatorname{Hom}_{S^{-1}C}(\Omega_{S^{-1}C/S^{-1}A}, S^{-1}M) \simeq \operatorname{Der}_{S^{-1}}(S^{-1}C, S^{-1}M)$$

and this completes the proof. □

2.19. *Module of derivations revisited.* We will be particularly interested in the setting in which $M = C$. In this case, we denote $\operatorname{Der}_A(C,C)$ simply as $\operatorname{Der}_A(C)$. It is a left C-submodule of $\operatorname{End}_A(C)$ and it is the dual of $\Omega_{C/A}$ via the canonical isomorphism

$$\operatorname{Der}_A(C) \cong \operatorname{Hom}_C(\Omega_{C/A}, C)$$

deduced from Proposition 2.13. However, $\operatorname{Der}_A(C)$ is not a (non-commutative) A-subalgebra of $\operatorname{End}_A(C)$ as the composition of derivations is not a derivation in general. Instead, there is also a Lie A-algebra structure on $\operatorname{End}_A(C)$ given by the bracket

$$[D, D'] := D \circ D' - D' \circ D, \quad \text{for each } D, D' \in \operatorname{End}_A(C).$$

With this structure, $\operatorname{Der}_A(C)$ is a Lie subalgebra of $\operatorname{End}_A(C)$ since $[D, D'] \in \operatorname{Der}_A(C)$ for all $D, D' \in \operatorname{Der}_A(C)$. In characteristic $p > 0$, for each $D \in \operatorname{Der}_A(C)$, the p-times composition D^p is also in $\operatorname{Der}_A(C)$. So $\operatorname{Der}_A(C)$ is a restricted Lie A-algebra (see [34, §1.1, Theorem 1]).

2.20. *Absolute derivations and absolute module of differentials.* Every ring C can be considered as a $\mathbb{Z}$-algebra. In this case, we denote $\operatorname{Der}(C) := \operatorname{Der}_{\mathbb{Z}}(C)$ and we call any derivation $D \in \operatorname{Der}(C)$ an *absolute derivation*, which is simply a ring map satisfying the Leibniz rule. We denote also $\Omega_C := \Omega_{C/\mathbb{Z}}$ and we call it the *absolute module of Kähler differentials* of C.

We include here a lemma on lifting absolute derivations from quotients rings that will be used later.

Lemma 2.21. *Let B be a ring such that Ω_B is projective as B-module. Let $C = B/I$ be a quotient ring, and let $\pi\colon B \to C$ be the quotient map. If $\delta \in \operatorname{Der}(C)$, then there exists $D \in \operatorname{Der}(B)$ such that $\pi \circ D = \delta \circ \pi$.*

Proof. Note that the composition $\delta \circ \pi\colon B \to C$ is a $\mathbb{Z}$-derivation. By Proposition 2.13, $\delta \circ \pi$ factorizes as $B \xrightarrow{d} \Omega_B \xrightarrow{\varphi} C$, where d is the absolute universal derivation of B and φ is some B-module homomorphism. That is, we have a commutative diagram

$$\begin{array}{ccc} B & \xrightarrow{\pi} & C \\ \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle \delta} \\ \Omega_B & \xrightarrow{\varphi} & C \end{array}$$

Since Ω_B is projective and π is surjective, there exists a B-module homomorphism $\Phi\colon \Omega_B \to B$ such that $\pi \circ \Phi = \varphi$, in other words, we have a commutative diagram

$$\begin{array}{ccccc} & & \Omega_B & & \\ & \overset{\Phi}{\swarrow} & \downarrow{\scriptstyle \varphi} & & \\ B & \xrightarrow{\pi} & C & \longrightarrow & 0\,. \end{array}$$

Then we consider the composition $D := \Phi \circ d$. By Proposition 2.13, we have that $D\colon B \to B$ is an absolute derivation and, using the equalities above, we show that it satisfies

$$\pi \circ D = \pi \circ \Phi \circ d = \varphi \circ d = \delta \circ \pi.$$

□

2.1.3. On p-basis

For this subsection, we restrict ourselves to the setting of rings of prime characteristic p. We recall the definition and some elementary properties of p-basis for ring extensions of exponent at most one, which can be found in [12, §3.1].

Definition 2.22. Let $A \subseteq C$ be a ring extension of exponent at most one and let $x_1, \ldots, x_n \in C$. The collection $\{x_1, \ldots, x_n\}$ is a *p-basis* for C over A if

(i) $x_1, \ldots, x_n$ generate C as A-algebra, i.e, $C = A[x_1, \ldots, x_n]$, and

(ii) $\{x_1, \ldots, x_n\}$ is a *p-independent set* over A, i.e., the set of *reduced monomials* $\{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} : 0 \leq \alpha_i < p\}$ is linearly independent over A.

By convention, in the trivial case, i.e, $A = C$, the empty set is the only p-basis, $n = 0$ and the set of reduced monomials is formed by the identity element $\{1_A\}$.

Remark 2.23. Let $A \subseteq C$ be a ring extension of exponent at most one. Then $\{x_1, \ldots, x_n\} \subset C$ is a p-basis for C over A if and only if C is a free A-module of rank p^n with basis the set of reduced monomials, or equivalently, if the A-algebra homomorphism $A[X_1, \ldots, X_n] \to C$ sending X_i into x_i induces an isomorphism

$$A[X_1, \ldots, X_n]/\langle X_1^p - x_1^p, \ldots, X_n^p - x_n^p \rangle \cong C.$$

The next example exhibits some remarkable ring extensions in which the existence of p-basis is guaranteed.

Example 2.24. It follows by Zorn's Lemma that every finite field extension of exponent one admits a p-basis. More generally, T. Kimura and H. Niitsuma proved in [40] that every exponent-one finite extension of regular local rings has a p-basis.

We include in the following lemma some well-known and useful properties of the p-basis. We do not explicit a proof as it is straightforward.

Lemma 2.25. *Let $A \subseteq C$ be a ring extension of exponent at most one.*

(1) If $\{x_1, \ldots, x_n\}$ is a p-basis for C over A, then for any $a_1, \ldots, a_n \in A$, the set $\{x_1 - a_1, \ldots, x_n - a_n\}$ is also a p-basis for C over A.

(2) Let A' be an A-algebra and set $C' := C \otimes_A A'$. If $\{x_1, \ldots, x_n\}$ is a p-basis for C over A, then $\{x_1 \otimes 1, \ldots, x_n \otimes 1\} \subset C'$ is a p-basis for C' over A'.

(3) Let B be an intermediate ring such that $A \subseteq B \subseteq C$. If $\{x_1, \ldots, x_r\}$ is a p-basis for C over B and $\{x_{r+1}, \ldots, x_n\}$ is a p-basis for B over A, then $\{x_1, \ldots, x_n\}$ is a p-basis for C over A.

We have a particular interest in the so called *splitting p-basis*, which induce an special presentation of the ring extension.

Definition 2.26. Let $A \subseteq C$ be a ring extension of exponent at most one. A *splitting p-basis* for C over A is a p-basis $\{x_1, \ldots, x_n\}$ such that $x_i^p = 0$ for all i. Equivalently, it is a p-basis that induces an A-algebra isomorphism $C \cong A[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$. By convention the empty set is also a splitting p-basis for any trivial extension.

We can obtain a splitting p-basis from an arbitrary p-basis by allowing a suitable base change if necessary.

Proposition 2.27. *Let $A \subseteq C$ be a ring extension with p-basis $\{x_1, \ldots, x_n\}$. Let $A \subseteq A'$ be a ring extension such that, for each $i = 1, \ldots, n$, there exists $y_i \in A'$ with $y_i^p = x_i^p$. Set $z_i := x_i \otimes 1 - 1 \otimes y_i \in C \otimes_A A'$. Then $\{z_1, \ldots, z_n\}$ is a splitting p-basis of $A' \subset C \otimes_A A'$.*

Proof. Let $C' := C \otimes_A A'$. By (2) in Lemma 2.25, we have that $\{x_1 \otimes 1, \ldots, x_n \otimes 1\}$ is a p-basis for C' over A'. For each $i = 1, \ldots, n$, we set $z_i := x_i \otimes 1 - 1 \otimes y_i \in C'$. Then, by (1) in Lemma 2.25, $\{z_1, \ldots, z_n\}$ is also a p-basis for C' over A'. Finally, since $x_i^p = y_i^p \in A$, we have $z_i^p = 0 \in C'$, so $\{z_1, \ldots, z_n\}$ is a splitting p-basis for C' over A'. □

Note that Proposition 2.27 applies for instance with $A' = C$ or just $A' = A$ if $A = A^p$. It also applies if $A = K$ is a field and $A' = L$ is any other field such that $K^{1/p} \subset L$. In particular, if K is an algebraically closed field, then any finite extension $K \subset C$ admitting a p-basis has a splitting p-basis.

Corollary 2.28. *Let $A \subseteq C$ be a ring extension of exponent at most one that admits a p-basis of n elements.*

(1) If $A = A^p$ (e.g., A a perfect field), then $C \cong A[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$ as A-algebras.

(2) $C \otimes_A C \cong C[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$ as (left) C-algebras.

2.1.4. Differentiably simple rings

In this subsection, we return to the general setting, where the rings are assumed to be commutative with unity and the characteristic will be specified in each case. We review some basic facts about differentiably simple rings, mainly of prime characteristic. In this context, we include here alternative proofs presented in [12, §2] for two important results: the characterization of Noetherian differentiably simple rings (Theorem 2.33), and a theorem describing the fiber of flat homomorphisms between Noetherian differentiably simple rings (Theorem 2.39).

Differentiably simple rings were introduced by E. Posner in [53]. He showed that these rings may be regarded as algebras over a field, which is indeed the differential centroid of the algebra. In the characteristic zero case, he proved that differentiably simple rings are always integral domains and that, under some finiteness conditions, they are integrally closed in its quotient field.

Definition 2.29. Let A be a ring. An ideal $I \subseteq A$ is *differential* if $D(I) \subseteq I$ for any absolute derivation $D\colon A \to A$. The ring A is *differentiably simple* if the only differential ideals are A and 0.

Example 2.30. It follows by definition that any field is a differentiably simple ring.

We are particularly interested in differentiably simple rings of prime characteristic p. The next proposition collects some basic facts of this type of rings.

Proposition 2.31 ([66, Theorem 2.1])**.** *Let A be a differentiably simple ring of prime characteristic p. Then*

(1) A is local and every element x in the maximal ideal satisfies $x^p = 0$.

(2) A^p is a field and every maximal subfield of A including A^p is a coefficient field.

Proof. Let $x \in A$ be a non-unit. Recall that any derivation of A is A^p-linear, so $\langle x^p \rangle \subset A$ is a proper differential ideal. Since A is differentiable simple, it must be $x^p = 0$. Thus, A is a local ring with maximal ideal $\mathfrak{m} = \{x \in A : x^p = 0\}$. Note also that A^p is a field, since any ideal of A^p extends to a differential ideal in A and the only differential ideals of A are 0 and A.

Let K be any maximal subfield of A including A^p. We show that A is a coefficient field, i.e., that the restriction to K of the quotient map $A \to A/\mathfrak{m}$ is surjective. If it is not, then there exists $x \in A$ such that $x - y \notin \mathfrak{m}$ for any $y \in K$. Let $a := x^p \in A^p \subseteq K$. Then the polynomial $X^p - a \in K[X]$ is irreducible. In fact, if $y \in K$ were a root, then $y^p = x^p$ and $(x - y)^p = 0$, which implies that $x - y \in \mathfrak{m}$, contradicting our choice of x. Thus, $K[X]/\langle X^p - a \rangle$ is a field. Since $K[x] \subset A$ is a quotient of $K[X]/\langle X^p - a \rangle$, we deduce that $K[x]$ is also a field. This contradicts the maximality of K. Thus, K must be a coefficient field. □

We show an example of a differentiably simple ring of characteristic p, which might not be Noetherian.

Example 2.32. Let K be a field of characteristic p and $\{X_\lambda\}_{\lambda\in\Lambda}$ a collection of variables that might not be finite. Then

$$C := K[X_\lambda : \lambda \in \Lambda]/\langle X_\lambda^p : \lambda \in \Lambda\rangle$$

is a differentiably simple ring. We make some simple observations to prove it:

(1) C is a local ring whose maximal ideal is generated by the class of the polynomials X_λ with $\lambda \in \Lambda$.

(2) It is clear that the partial derivatives $\frac{\partial}{\partial X_\lambda}$ of $K[X_\lambda : \lambda \in \Lambda]$ preserve the ideal $\langle X_\lambda^p : \lambda \in \Lambda\rangle$. Hence, they induce derivations $\delta_\lambda \colon C \to C$.

(3) The class in C of a polynomial $f \in K[X_\lambda : \lambda \in \Lambda]$ is a unit if and only if the constant term of f is non-zero.

Let $I \subset C$ be a proper differential ideal. Assume that $I \neq 0$. Then there is $f \in K[X_\lambda : \lambda \in \Lambda]$ included in the ideal $\langle X_\lambda : \lambda \in \Lambda\rangle$, but not in the ideal $\langle X_\lambda^p : \lambda \in \Lambda\rangle$, whose class in C belongs to I. Note that the condition $f \notin \langle X_\lambda^p : \lambda \in \Lambda\rangle$ implies that f has a non-zero term $cX_{\lambda_1}^{\alpha_1}\cdots X_{\lambda_n}^{\alpha_n}$ with $c \in K$ and $0 \leq \alpha_i < p$ for $i = 1, \ldots, n$. We consider the composition of partial derivatives

$$D := \frac{\partial^{\beta_1}}{\partial X_{\lambda_1}^{\beta_1}} \circ \cdots \circ \frac{\partial^{\beta_n}}{\partial X_{\lambda_n}^{\beta_n}}\,.$$

Then D transforms f into a polynomial $D(f)$ whose constant term is $\beta_1!\cdots\beta_n!\cdot c \neq 0$. By (2), D induces a derivation on C, whose evaluation at the class of f coincides with the class of $D(f)$. By (3), we conclude that the class of f is a unit, and this contradicts the fact that I is a proper ideal. Thus, I must be zero.

In prime characteristic, L. R. Harper determined the structure of finite dimensional differentiably simple algebras over an algebraically closed field ([29]). He showed that these rings are isomorphic to a truncated polynomial algebra. Later, this result was extended to more general settings by S. Yuan ([66]) and R. E. Block ([6], [7]). The original proofs of L. R. Harper and S. Yuan involve elaborated computations with derivations. More recently, shorter proofs were obtained by A. K. Maloo ([46]) and V. V. Bavula ([4]). We include here our alternative proof presented in [12, Theorem 2.4] for the characterization of Noetherian differentiably simple rings of prime characteristic. The statement for this characterization makes use of Proposition 2.31.

Theorem 2.33 (Harper). *Let A be a Noetherian differentiably simple ring of characteristic p. Let $\{x_1, \ldots, x_n\}$ be a minimal generating set for the maximal ideal and $K \subseteq A$ a coefficient field. Then there is an isomorphism of K-algebras*

$$K[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p\rangle \simeq A$$

induced by the homomorphism $K[X_1, \ldots, X_n] \to A$ given by $X_i \mapsto x_i$.

Proof. Let $\pi\colon K[X_1,\dots,X_n] \to A$ be the K-algebra homomorphism given by $X_i \mapsto x_i$ and let $I := \ker(\pi)$. Since K is a coefficient field for A, we have by Proposition 2.31 that $A = K + \mathfrak{m}$. Since $\{x_1,\dots,x_n\}$ is a minimal generating set for $\mathfrak{m}$, the map π is surjective. Recall that $x^p = 0$ for all $x \in \mathfrak{m}$ by Proposition 2.31, so $\langle X_1^p,\dots,X_n^p\rangle \subseteq I$. Thus, it only remains to check the reverse inclusion to obtain the isomorphism of the statement.

Since $\{x_1,\dots,x_n\}$ is a minimal generating set for the maximal ideal $\mathfrak{m}$, its image in $\mathfrak{m}/\mathfrak{m}^2$ induce a basis as K-vector space and $\pi(I) \subseteq \mathfrak{m}^2$. Then it follows that $I \subseteq \langle X_1,\dots,X_n\rangle^2$. We denote by J the ideal generated by I and all the evaluations $D(f)$ for $f \in I$ and $D \in \mathrm{Der}(K[X_1,\dots,X_n])$. We show that $J \subseteq \langle X_1,\dots,X_n\rangle$. Note that the elements in I are K-linear combinations of elements of the form $g \cdot X_iX_j$ for some $g \in K[X_1,\dots,X_n]$ and $i,j \in \{1,\dots,n\}$. In addition, for every derivation $D \in \mathrm{Der}(K[X_1,\dots,X_n])$, we have

$$D(g \cdot X_iX_j) = g \cdot X_iD(X_j) + g \cdot X_jD(X_i) + X_iX_jD(g),$$

by an application of the Leibnitz's rule. Since the derivations are additive maps, it is clear that J is generated by elements in $\langle X_1,\dots,X_n\rangle$. Thus, $J \subseteq \langle X_1,\dots,X_n\rangle$ and $\pi(J)$ is a proper ideal of A.

We claim that $\pi(J)$ is a differential ideal of A. We have to show that there is an inclusion $\delta(\pi(J)) \subseteq \pi(J)$ for any $\delta \in \mathrm{Der}(A)$. We can apply Lemma 2.21 with $B = K[X_1,\dots,X_n]$ and $C = B/I = A$, since Ω_B is free (see [44, Example 2.5.(d)]). So there exists $D \in \mathrm{Der}(K[X_1,\dots,X_n])$ such that $\pi \circ D = \delta \circ \pi$. Then the claim follows if we prove that $D(J) \subseteq J$, equivalently, if we prove that $D(g) \in J$ for all g in a generating set for J, that is, if we prove that $D(f), D(E(f)) \in J$ for all $f \in I$ and $E \in \mathrm{Der}(K[X_1,\dots,X_n])$. On the one hand, we have $\pi(D(I)) = \delta(\pi(I)) = 0$ because $I = \ker(\pi)$, so $D(I) \subseteq I \subseteq J$. On the other hand, for any $E \in \mathrm{Der}(K[X_1,\dots,X_n])$ and $f \in I$, we have $D(E(f)) = E(D(f)) - [E,D](f)$. Note that $D(f)$ belongs to I, by the previous observation. Then $E(D(f)), [E,D](f) \in J$ since $E, [E,D] \in \mathrm{Der}(K[X_1,\dots,X_n])$. Hence, $D(E(f)) \in J$ as we wanted.

Finally, as A is assumed to be differentiably simple and $\pi(J)$ is a proper differential ideal, we have $\pi(J) = 0$. Then $I = J$ and so $I \subseteq \langle X_1,\dots,X_n\rangle$. Assume that there is $f \in I$ such that $f \notin \langle X_1^p,\dots,X_n^p\rangle$. Then, as we proved in Example 2.32, there exists $D \in \mathrm{Der}(K[X_1,\dots,X_n])$ such that $D(f)$ is a polynomial with a non-zero constant term. Thus, $\pi(D(f)) \neq 0$, but this is a contradiction since $D(f) \in J$. Therefore, we necessarily have $I \subseteq \langle X_1^p,\dots,X_n^p\rangle$ and the proof of the theorem is complete. □

Remark 2.34. Any Noetherian differentiably simple ring A of characteristic p is a (zero-dimensional) complete intersection. In fact, by Theorem 2.33, we have an isomorphism

$$A \simeq K[X_1,\dots,X_n]/\langle X_1^p,\dots,X_n^p\rangle \simeq K[[X_1,\dots,X_n]]_{\langle X_1,\dots,X_n\rangle}/\langle X_1^p,\dots,X_n^p\rangle.$$

As a corollary of Harper's Theorem we obtain the next result that will be used in the proof of Theorem 2.39 on the fiber of flat homomorphisms between Noetherian differentiably simple rings of characteristic p.

Corollary 2.35. *Let $(A,\mathfrak{m})$ be a Noetherian differentiably simple ring of characteristic p and let $f \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then* $\mathrm{ann}_A(f) = f^{p-1}A$.

Proof. By Theorem 2.33, we may assume that $A = K[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$ for some coefficient field $K \subseteq A$ and that the classes of $X_1, \ldots, X_n$ are a minimal generating set for the maximal ideal $\mathfrak{m}$. Observe that $f \in \mathfrak{m} \setminus \mathfrak{m}^2$ is the class of a polynomial from $K[X_1, \ldots, X_n]$ with no constant term and that has a monomial term of degree one. After a suitable change of variables, we may assume that f is the class of X_1. Let $A' := K[X_1]/\langle X_1^p \rangle \subseteq A$. Note that A is flat as A'-module and that $\operatorname{ann}_{A'}(f) = f^{p-1}A'$. Then, by Lemma A.22, we have $\operatorname{ann}_A(f) = \operatorname{ann}_{A'}(f)A = f^{p-1}A$. □

We continue with the study of Noetherian differentiably simple rings of prime characteristic. In particular, we describe in the following proposition the quotients of those rings that are differentiably simple too. This proposition can be deduced also from the main result of [46], which describes the maximal differential ideals of a Noetherian local ring.

Proposition 2.36. *Let $(A, \mathfrak{m})$ be a Noetherian differentiably simple ring of characteristic p. For any proper ideal $I \subset A$, the quotient ring A/I is differentiably simple if and only if I is generated by part of a minimal system of generators of $\mathfrak{m}$.*

Proof. Let $K \subseteq A$ be a coefficient field and $I \subset A$ a proper ideal. First, we suppose that I is generated by part of a minimal generating set for $\mathfrak{m}$. By Theorem 2.33, we may assume that $A = K[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$ and that I is the ideal generated by the classes of $X_1, \ldots, X_r$ for some $r \leq n$. If $r = n$, then $A/I \simeq K$, and if $r < n$, we have $A/I \simeq K[X_{r+1}, \ldots, X_n]/\langle X_{r+1}^p, \ldots, X_n^p \rangle$. In both cases, A/I is differentiably simple, as we have shown in Example 2.32.

Conversely, we assume that A/I is differentiably simple. We consider the exact sequence of K-vector spaces

$$0 \to (I + \mathfrak{m}^2)/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}/(I + \mathfrak{m}^2) \to 0.$$

Note that it is split exact, so $\mathfrak{m}/\mathfrak{m}^2 \simeq ((I + \mathfrak{m}^2)/\mathfrak{m}^2) \oplus (\mathfrak{m}/(I + \mathfrak{m}^2))$. Then we can take $x_1, \ldots, x_r \in I$, whose classes modulo $\mathfrak{m}^2$ form a basis for the K-vector space $(I + \mathfrak{m}^2)/\mathfrak{m}^2$, and $x_{r+1}, \ldots, x_n \in \mathfrak{m}$ whose classes modulo $I + \mathfrak{m}^2$ form a basis for the K-vector space $\mathfrak{m}/(I + \mathfrak{m}^2)$. Hence, the classes of $x_1, \ldots, x_n \in \mathfrak{m}$ modulo $\mathfrak{m}^2$ form a basis for $\mathfrak{m}/\mathfrak{m}^2$. By the local version of Nakayama's Lemma (Corollary A.35), we deduce that $\{x_1, \ldots, x_n\}$ is a minimal generating set for $\mathfrak{m}$, and that $x_{r+1}, \ldots, x_n$ induce a minimal generating set for $\mathfrak{m}/I \subset A/I$. The way in which we have chosen the generating system gives us a commutative diagram of homomorphisms of K-algebras

$$\begin{array}{ccc} K[X_1, \ldots, X_n] & \xrightarrow{\varphi} & K[X_{r+1}, \ldots, X_n] \,, \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \bar{\pi}} \\ A & \xrightarrow{\qquad \bar{\varphi} \qquad} & A/I \end{array}$$

where $\pi(X_i) = x_i$ for $i = 1, \ldots, n$, $\bar{\pi}(X_i) = x_i + I$ for $i = r+1, \ldots, n$, φ is the quotient map with kernel $\langle X_1, \ldots, X_r \rangle$ and $\bar{\varphi}$ is the obvious quotient map. Since A/I is differentiably simple, $\bar{\pi}$ is the surjective homomorphism from Theorem 2.33 and we

have $\ker(\bar{\pi}) = \langle X_{r+1}^p, \ldots, X_n^p \rangle$. From the commutativity of the diagram, we deduce that

$$\pi^{-1}(I) = \pi^{-1}(\ker(\bar{\varphi})) = \varphi^{-1}(\ker(\bar{\pi})) = \langle X_1, \ldots, X_r, X_{r+1}^p, \ldots, X_n^p \rangle.$$

Therefore, $I = \langle x_1, \ldots, x_r \rangle$ and, in particular, it is generated by part of a minimal generating set for $\mathfrak{m}$. □

The fact stated in the following proposition was used by M. André in [1] to prove part of Theorem 2.39 on the fiber of flat homomorphisms between Noetherian differentiably simple rings of characteristic p. The argument included in the proof appeared already in the proof of S. Yuan for [66, Theorem 11].

Proposition 2.37. *Let C be a differentiably simple ring, not necessarily of characteristic p. Let $A \subseteq C$ be a subring such that C is a free A-module. Then A is also differentiably simple.*

Proof. Let I be a differential ideal of A. We prove that either $I = A$ or $I = 0$. We first show that the extended ideal IC is a differential ideal of C. Let $D\colon C \to C$ be any absolute derivation and let $\{x_\lambda : \lambda \in \Lambda\}$ be a basis for C as A-module. Then there are additive maps $D_\lambda\colon A \to A$ such that $D(a) = \sum_{\lambda \in \Lambda} D_\lambda(a) x_\lambda$ for all $a \in A$. In fact, each D_λ is an absolute derivation of A. Since I is a differential ideal, $D_\lambda(I) \subseteq I$ for all $\lambda \in \Lambda$. Then it follows that $D(I) \subseteq IC$, and so $D(IC) \subseteq IC$, as we wanted to show. As C is differentiably simple, we have that $IC = C$ or $IC = 0$. Finally, since C is a free A-module, it is in particular faithfully flat, so we conclude that either $I = A$ or $I = 0$. □

We recall the next proposition from E. Kunz on complete intersection rings that will be used in the demonstration of Theorem 2.39. The proof for this fact follows from the main result in [43], which is based on a theorem of T. Gulliksen ([28, Proposition 1.4.9]). However, E. Kunz also presented an alternative proof of his main result by using just the main technique in the proof of T. Gulliksen's theorem, which is J. Tate's method of adjoining variables to kill cycles ([63]).

Proposition 2.38 ([43, Proposition 3.3])**.** *Let A be a complete intersection ring and let $x \in A$ be a non-zero element. Then* $\operatorname{ann}(x)$ *is a principal ideal if and only if the quotient ring $A/\langle x \rangle$ is a complete intersection.*

Finally, we prove Theorem 2.39 that describes the fiber of flat homomorphisms between Noetherian differentiably simple rings of characteristic p. The key point in our proof is to establish that some ring is a complete intersection. Our proof is different from the one given in [1], which relies on a very strong result of L. L. Avramov ([3, Theorem 1.1]) about the homology of a general local flat extension.

Theorem 2.39 ([1, Proposition 67])**.** *Let $(A, \mathfrak{m}_A) \to (C, \mathfrak{m}_C)$ be a flat local homomorphism of Noetherian local rings of exponent one. If C is differentiably simple, then so are A and $C/\mathfrak{m}_A C$.*

Proof. Since C is differentiably simple, we have that $x^p = 0$ for all $x \in \mathfrak{m}_X$ by Proposition 2.31. In particular, we have $x^p = 0$ for any $x \in \mathfrak{m}_A$, so $\mathfrak{m}_A$ is nilpotent. Then A is Artinian, by Proposition A.5, and flatness of C over A implies that C is free as A-module, by Corollary A.37. Therefore, we are under the hypothesis of Proposition 2.37 and we conclude that A is differentiably simple.

Now, we prove that $C/\mathfrak{m}_A C$ is differentiably simple by induction on the embedding dimension of A. If $\operatorname{embdim}(A) = 0$, then $\mathfrak{m}_A = 0$. Thus, $\mathfrak{m}_A C = 0$ and $C/\mathfrak{m}_A C = C$ which is differentiably simple by hypothesis. We assume now that $\operatorname{embdim}(A) > 0$, so we can choose $f \in \mathfrak{m}_A \setminus \mathfrak{m}_A^2$. We claim that $f \in \mathfrak{m}_C \setminus \mathfrak{m}_C^2$.

By Theorem 2.33, we have an isomorphism $C \simeq K[[X_1, \ldots, X_n]]/\langle X_1^p, \ldots, X_n^p\rangle$ for some coefficient field $K \subseteq C$. In particular, C is a (zero-dimensional) complete intersection ring as we noted in Remark 2.34. By an application of Corollary 2.35 to the local ring $(A, \mathfrak{m}_A)$ and $f \in \mathfrak{m}_A \setminus \mathfrak{m}_A^2$, we have $\operatorname{ann}_A(f) = f^{p-1}A$. Since $A \to C$ is flat, we also have by Lemma A.22 that $\operatorname{ann}_C(f) = f^{p-1}C$ is a principal ideal. Then we can apply Proposition 2.38 to conclude that the quotient ring $C/\langle f\rangle$ is also a complete intersection of dimension zero.

Let $F \in K[[X_1, \ldots, X_n]]$ be a representative of $f \in C$. So

$$C/\langle f\rangle \simeq K[[X_1, \ldots, X_n]]/\langle X_1^p, \ldots, X_n^p, F\rangle.$$

Note that the ideal $\langle X_1^p, \ldots, X_n^p, F\rangle$ is minimally generated by n elements which can be chosen among the previous $n+1$ generators. We claim that F is one of these generators. In other case, F is generated by $X_1^p, \ldots, X_n^p$ and $f = 0 \in C$. Observe that $A \to C$ is injective, since it is a flat homomorphism between local rings (see Corollary A.20). So we would have $f = 0 \in A$, which contradicts $f \notin \mathfrak{m}_A^2$. Without loss of generality, we may assume that $\langle X_1^p, \ldots, X_n^p, F\rangle$ is minimally generated by $X_2^p, \ldots, X_n^p, F$. Then

$$X_1^p = GF + H_2 X_2^p + \cdots + H_n X_n^p$$

for some $G, H_2, \ldots, H_n \in K[[X_1, \ldots, X_n]]$. Using that $\operatorname{ann}_C(f) = f^{p-1}C$, we deduce that

$$G = UF^{p-1} + U_1 X_1^p + U_2 X_2^p + \ldots + U_n X_n^p$$

for some $U, U_1, \ldots, U_n \in K[[X_1, \ldots, X_n]]$. Then $X_1^p \in \langle F^p, FX_1^p, X_2^p, \ldots, X_n^p\rangle$. This implies that necessarily $F \in \langle X_1, \ldots, X_n\rangle \setminus \langle X_1, \ldots, X_n\rangle^2$. Hence $f \in \mathfrak{m}_C \setminus \mathfrak{m}_C^2$ and this proves the claim.

Finally, we set $\bar{A} := A/fA$ and $\bar{C} := C/fC$, which are Noetherian rings by Proposition A.3. The induced extension $\bar{A} \to \bar{C}$ is a flat local homomorphism of Noetherian local rings of exponent one such that $\bar{C}$ is differentiably simple by Proposition 2.36. Since $\operatorname{embdim}(\bar{A}) < \operatorname{embdim}(A)$, the inductive hypothesis implies that $\bar{C}/\mathfrak{m}_{\bar{A}}\bar{C}$ is differentiably simple. As there is an isomorphism $\bar{C}/\mathfrak{m}_{\bar{A}}\bar{C} \cong C/\mathfrak{m}_A C$, we conclude that $C/\mathfrak{m}_A C$ is differentiably simple. □

Corollary 2.40. *Let $(A, \mathfrak{m}_A) \to (C, \mathfrak{m}_C)$ be a flat extension of Noetherian differentiably simple rings of exponent one. Then any minimal generating set for the maximal ideal of A can be extended to a minimal generating set for the maximal ideal of C.*

Proof. Let $\{x_1, \ldots, x_r\}$ be a minimal generating set for $\mathfrak{m}_A$. Since $A \to C$ is flat, $\{x_1, \ldots, x_r\}$ is also a minimal generating set for the extended ideal $\mathfrak{m}_A C$. Since C is differentiably simple, the fiber $C/\mathfrak{m}_A C$ is differentiably simple by Theorem 2.39. It follows from Proposition 2.36 that $\mathfrak{m}_A C$ is generated by part of a minimal generating set for $\mathfrak{m}_C$. Since $\{x_1, \ldots, x_r\}$ is a minimal generating set for $\mathfrak{m}_A C \subseteq \mathfrak{m}_C$ and since any two minimal generating sets must have the same length, we conclude that $\{x_1, \ldots, x_r\}$ is part of minimal generating set for $\mathfrak{m}_C$. □

2.2. Galois extensions of rings

In this section, all the rings are assumed to have characteristic p. We begin with the original definition of Galois extensions of exponent one given by S. Yuan in [68] and some properties that are immediately deduced from it. Then we study the relation of these extensions with differentiably simple rings (Subsection 2.2.1), the modules of Kähler differentials (Subsection 2.2.2) and the modules of derivations (Subsection 2.2.3). We show that Galois extensions coincide with purely inseparable extensions of exponent one and we conclude with a compilation of characterizations of Galois extensions (Subsection 2.2.4).

Definition 2.41. A finite extension of rings $A \subseteq C$ is a *Galois extension of exponent one* if the following conditions hold:

(i) $A \subseteq C$ has exponent at most one, i.e., $C^p \subseteq A$,

(ii) C is a projective A-module, and

(iii) for each prime ideal $\mathfrak{p} \subset A$, the extension $A_\mathfrak{p} \subseteq C_\mathfrak{p} := C \otimes_A A_\mathfrak{p}$ admits a p-basis.

Note that a trivial extension, i.e., $A = C$, is considered a Galois extension of exponent one, because trivial extensions are considered to have a p-basis (see Definition 2.22).

Remark 2.42. In the above definition, condition (i) on having exponent at most one is redundant. Indeed, condition (iii) implies that $\exp(C_\mathfrak{p}/A_\mathfrak{p}) \leq 1$ for every prime $\mathfrak{p} \subset A$. Thus, $\exp(C/A) \leq 1$ by Lemma 2.10.

Remark 2.43. Note that condition (iii) in the above definition already implies that $C_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module for all prime ideal $\mathfrak{p} \subset A$ (see Remark 2.23). Then, by Proposition 1.7, condition (ii) in the definition of Galois extension can be replaced by the condition that C is an A-module of finite presentation.

Remark 2.44. Observe that condition (iii) in the definition of Galois extension only needs to be verified at maximal ideals. In fact, assume that $A_\mathfrak{m} \subseteq C_\mathfrak{m}$ admits a p-basis for any maximal ideal $\mathfrak{m} \subset A$. Given a prime ideal $\mathfrak{p} \subset A$, there is a maximal ideal such that $\mathfrak{p} \subseteq \mathfrak{m}$. The extension $A_\mathfrak{p} \subseteq C_\mathfrak{p}$ coincides with the base change of $A_\mathfrak{m} \subseteq C_\mathfrak{m}$ via the localization map $A_\mathfrak{m} \to A_\mathfrak{p}$. Thus, $A_\mathfrak{p} \subseteq C_\mathfrak{p}$ has a p-basis by Lemma 2.25.(2).

Galois extensions behave well under base extension and under composition when restricted to exponent one extensions. We collect these properties in the following lemma, which is a consequence of Lemma 2.25.

Lemma 2.45. *Let $A \subseteq C$ be a finite extension of rings of exponent at most one.*

(1) If $A \subseteq C$ has a p-basis, then $A \subseteq C$ is a Galois extension.

(2) Let A' be an A-algebra. If $A \subseteq C$ is Galois extension, then $A' \subseteq C \otimes_A A'$ is also Galois.

(3) Let B be an intermediate subring such that $A \subseteq B \subseteq C$. If $A \subseteq B$ and $B \subseteq C$ are Galois extensions, then $A \subseteq C$ is also a Galois extension.

Proof. We assume first that $A \subseteq C$ has a p-basis to prove (1). Then C is a free A-module of finite rank as we noted in Remark 2.23. In particular, C is projective as A-module. Since $A \subseteq C$ has a p-basis, for every prime ideal $\mathfrak{p} \subset A$, the extension $A_\mathfrak{p} \subseteq C_\mathfrak{p} := C \otimes_A A_\mathfrak{p}$ obtained by the base change $A \to A_\mathfrak{p}$ also admits a p-basis by Lemma 2.25.(2).

We suppose now that $A \subseteq C$ is a Galois extension to demonstrate (2). Let $C' := C \otimes_A A'$. Since $A \subseteq C$ is a finite projective ring extension, we have that $A' \subseteq C'$ is also a finite extension such that C' is projective as A'-module by Remark 1.16. Then, by Remark 2.42, to show that $A' \subseteq C'$ is Galois it only lefts to show that for any prime ideal $\mathfrak{q} \subset A'$, the extension $A'_\mathfrak{q} \subseteq C'_\mathfrak{q}$ has a p-basis. Recall that there is a morphism $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$ induced by $A \to A'$. Given a prime ideal $\mathfrak{q} \subset A'$, let $\mathfrak{p} \subset A$ be the prime ideal such that $\mathfrak{q} \mapsto \mathfrak{p}$ via the previous morphism. Hence, we have natural maps $A_\mathfrak{p} \to A_\mathfrak{p} \otimes_A A' \to A'_\mathfrak{q}$. Then, by Lemma 2.25.(2), the p-basis for $C_\mathfrak{p}$ over $A_\mathfrak{p}$ induces a p-basis for $C'_\mathfrak{q}$ over $A'_\mathfrak{q}$ as we wanted.

Finally, to prove (3) we take an intermediate subring B such that both $A \subseteq B$ and $B \subseteq C$ are Galois. Since C is a projective as B-module and $A \hookrightarrow B$ is a ring homomorphism such that B is projective as A-module, we have that C is also projective as A-module by Proposition 1.5. Since $A \subseteq C$ is a finite extension of exponent at most one, in order to show that $A \subseteq C$ is Galois, it only lefts to check that $C_\mathfrak{p}$ has a p-basis over $A_\mathfrak{p}$ for every prime ideal $\mathfrak{p} \subset A$. We have natural identifications $\mathrm{Spec}(A) \simeq \mathrm{Spec}(B) \simeq \mathrm{Spec}(C)$ (see Remark 2.2). Then for each prime ideal $\mathfrak{p} \subset A$, we have a p-basis for $B_\mathfrak{p}$ over $A_\mathfrak{p}$ and for $C_\mathfrak{p}$ over $B_\mathfrak{p}$. Then by Lemma 2.25.(3), we conclude that $C_\mathfrak{p}$ has a p-basis over $A_\mathfrak{p}$, as we wanted. □

2.2.1. Galois extensions and differentiably simple rings

In this subsection, we establish a characterization of Galois extensions of exponent one using differentiably simple rings as we do in [12, §3.1]. The next proposition relates this notion with p-basis over a field.

Proposition 2.46. *Let $K \subseteq C$ be a finite extension of exponent at most one such that K is a field. Then C has p-basis over K if and only if C is differentiably simple.*

Proof. If C has p-basis over K, then by Proposition 2.27 we have an isomorphism

$$C \otimes_K K^{1/p} \simeq K^{1/p}[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$$

for some n. As we showed in Example 2.32, the above ring is differentiably simple. Since $K^{1/p}$ is a free K-module, $C \otimes_K K^{1/p}$ is also a free C-module by Proposition A.32. Thus, since $C \otimes_K K^{1/p}$ is a differentiably simple ring such that $C \subseteq C \otimes_K K^{1/p}$ and $C \otimes_K K^{1/p}$ is a free C-module, we conclude by Proposition 2.37 that C is differentiably simple.

We assume now that C is differentiably simple. Note that C is Noetherian since it has finite dimension as K-vector space (Proposition A.4). Since $K \subseteq C$ has exponent at most one, we have $C^p \subseteq K$ and there is a coefficient field $L \subseteq C$ that contains K by Proposition 2.31. Then there is an isomorphism of L-algebras $C \cong L[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$ by Theorem 2.33. It is clear that the the classes of $X_1, \ldots, X_n$ form a p-basis for C over L and L has also a p-basis over K since $K \subseteq L$ is a field extension (see Example 2.24). Thus, C has a p-basis over K by (3) in Lemma 2.45. □

Using the previous proposition, we extend the relation between p-basis and differentiably simple rings to the context of flat finite extensions of local rings with exponent one.

Proposition 2.47. *Let $(A, \mathfrak{m}_A) \subseteq (C, \mathfrak{m}_C)$ be a finite flat extension of exponent at most one between local rings. Then the following conditions are equivalent:*

(1) C has a p-basis over A.

(2) $C/\mathfrak{m}_A C$ has a p-basis over $\kappa(A) := A/\mathfrak{m}_A$.

(3) $C/\mathfrak{m}_A C$ is a differentiably simple ring.

Proof. If C has a p-basis over A, then $C/\mathfrak{m}_A C = C \otimes_A (A/\mathfrak{m}_A)$ has a p-basis over $A/\mathfrak{m}_A$ by Lemma 2.45.(2). This proves the implication (1)⇒(2). Note that the equivalence (2)⇔(3) follows by Proposition 2.46. Thus, it remains to show that (2)⇒(1). Since C is finite and flat over the local ring A, it is a free A-module of finite rank (Corollary A.37). We choose $x_1, \ldots, x_n \in C$ whose classes module $\mathfrak{m}_A C$ form a p-basis for $C/\mathfrak{m}_A C$ over $\kappa(A)$. Then the classes in $C/\mathfrak{m}_A C$ of the reduced monomials form a basis for $C/\mathfrak{m}_A C$ as a $\kappa(A)$-vector space. As a consequence of Nakayama's Lemma (see Proposition A.36), the reduced monomials on $x_1, \ldots, x_n$ form a basis for C as free A-module. Thus, $\{x_1, \ldots, x_n\}$ is a p-basis for C over A. □

Finally, we deduce immediately from the above proposition a characterization of Galois extensions in terms of differentiably simple rings.

Corollary 2.48 ([44, Theorem 15.5])**.** *Let $A \subseteq C$ be a finite ring extension of exponent at most one such that C is projective as a A-module. Then $A \subseteq C$ is Galois if and only if $C_\mathfrak{p}/\mathfrak{p}C_\mathfrak{p}$ is differentiably simple for each prime ideal $\mathfrak{p} \subset A$.*

Furthermore, using Proposition 2.47, we can characterize Galois extensions among finite projective extensions of finite exponent as flat families of Galois extensions.

Corollary 2.49. *Let $A \subseteq C$ be a finite ring extension of exponent at most one such that C is projective as A-module. Then $A \subseteq C$ is Galois if and only if $A/\mathfrak{m} \subseteq C/\mathfrak{m}C$ is Galois for every maximal ideal $\mathfrak{m} \subset A$.*

Proof. If $A \subseteq C$ is Galois, the extension $A/\mathfrak{m} \subseteq C/\mathfrak{m}C$ that results from the base change $A \to A/\mathfrak{m}A$ is Galois by Lemma 2.45.(2). Conversely, assume that $A/\mathfrak{m} \subseteq C/\mathfrak{m}C$ is Galois for every maximal ideal $\mathfrak{m} \subset A$. By Remark 2.44, we only have to show that $A_\mathfrak{m} \subseteq C_\mathfrak{m}$ has a p-basis. Note that $A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} \simeq A/\mathfrak{m}$, since localization and taking the quotient commute. Then $A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} \subseteq C_\mathfrak{m}/\mathfrak{m}C_\mathfrak{m}$ has a p-basis, since $A/\mathfrak{m} \subseteq C/\mathfrak{m}C$ is Galois. By Proposition 2.47, this implies that $C_\mathfrak{m}$ has a p-basis over $A_\mathfrak{m}$. □

2.2.2. Galois extensions and the module of differentials

In this subsection, we characterize Galois extensions of exponent one in terms of the modules of Kähler differentials. With this aim, we review the notion of *differential basis* in relation to the notion of p-basis. We recover here some ideas from [44, §5] and our perspective from [11, §3]. The particular case of finite extensions of exponent one between regular local rings was previously treated by T. Kimura and H. Niitsuma in [41].

Definition 2.50. Let C be a finitely generated A-algebra and let $x_1, \ldots, x_n \in C$. The collection $\{x_1, \ldots, x_n\}$ is a *differential basis* if $\Omega_{C/A}$ is a free C-module with basis $\{dx_1, \ldots, dx_n\}$. By convention, the empty set is considered a differential basis if $C = A$.

We use the next technical lemma to study the relation between p-basis and differential basis.

Lemma 2.51. *Let $A \subseteq C$ be a finite extension of rings of finite exponent. If $\Omega_{C/A} = 0$, then $C = A$.*

Proof. By Lemma A.9, the equality $C = A$ holds if and only if $C_\mathfrak{p} = A_\mathfrak{p}$ for every prime ideal $\mathfrak{p} \subset A$. Since C is a finite A-module, by the local version of Nakayama's Lemma (see Lemma A.35) it is enough to prove that the inclusion $\kappa(\mathfrak{p}) \hookrightarrow C \otimes_A \kappa(\mathfrak{p})$ is an equality for each prime ideal $\mathfrak{p} \subset A$. Hence, we may assume that A is a field K.

Under these assumptions, C is a finite K-algebra such that $C^{p^e} \subseteq K$ for some $e \geq 0$ and $\Omega_{C/K} = 0$. In particular, it follows from the homeomorphism in Remark 2.2 that C is local. We have to prove that $C = K$. Let $\mathfrak{m}$ be the maximal ideal and $L := C/\mathfrak{m}$ be the residue field of C. By Proposition 2.15, the second fundamental exact sequence is

$$\mathfrak{m}/\mathfrak{m}^2 \to L \otimes_C \Omega_{C/K} \to \Omega_{L/K} \to 0.$$

Then $\Omega_{C/K} = 0$ implies that $\Omega_{L/K} = 0$. Since $L^{p^e} \subseteq K$, it follows by [44, Proposition 5.7.(c)] that $L = K$. Therefore, since $K \subset C$, the exact sequence

$$0 \to \mathfrak{m} \to C \to L \to 0$$

splits, and $C = K \oplus \mathfrak{m}$. We consider the map $D\colon C \to \mathfrak{m}/\mathfrak{m}^2$ that results from the composition of the projection $C \to \mathfrak{m}$ followed by the quotient map $\mathfrak{m} \to \mathfrak{m}/\mathfrak{m}^2$. It is easy to show that D is a surjective K-derivation from C to $\mathfrak{m}/\mathfrak{m}^2$. Recall from Proposition 2.13 that $\mathrm{Der}_K(C, \mathfrak{m}/\mathfrak{m}^2) \cong \mathrm{Hom}_C(\Omega_{C/K}, \mathfrak{m}/\mathfrak{m}^2)$. Then, since $\Omega_{C/K} = 0$, it must be $D = 0$. Since D is surjective, we have $\mathfrak{m} = \mathfrak{m}^2$. Finally, by Nakayama's Lemma (see (1) in Lemma A.34), we conclude that $\mathfrak{m} = 0$. Therefore, $C = K$ as we wanted. □

We show in the following lemma that the generators of an algebra over a ring are closely related to the generators of its module of differentials.

Lemma 2.52. *Let $A \subseteq C$ be a finite extension of rings of finite exponent. Let $x_1, \dots, x_n \in C$. Then $C = A[x_1, \dots, x_n]$ if and only if $dx_1, \dots, dx_n$ generate $\Omega_{C/A}$ as C-module. In particular, the minimum number of generators of C as A-algebra is the same as the minimum number of generators of $\Omega_{C/A}$ as C-module.*

Proof. Recall that $\Omega_{C/A}$ is generated by $\{dc\colon c \in C\}$ as C-module. In particular, if $C = A[x_1, \dots, x_n]$, applying the Leibniz rule it follows that $dx_1, \dots, dx_n$ generate $\Omega_{C/A}$ as C-module.

Conversely, we assume that $dx_1, \dots, dx_n$ generate $\Omega_{C/A}$ as C-module and set $C' := A[x_1, \dots, x_n]$. In this case, the first fundamental exact sequence from Proposition 2.14 is

$$C \otimes_{C'} \Omega_{C'/A} \to \Omega_{C/A} \to \Omega_{C/C'} \to 0.$$

Then, by the previous argument, $dx_1, \dots, dx_n$ also generate $\Omega_{C'/A}$ as C'-module and $C \otimes_{C'} \Omega_{C'/A} \to \Omega_{C/A}$ is surjective. Hence, we deduce that $\Omega_{C/C'} = 0$. Since $C' \subseteq C$ is a finite extension such that $C'^{p^e} \subseteq C$ for some $e \geq 0$, we can apply Lemma 2.51 to conclude that $C = C'$. Therefore, $x_1, \dots, x_n$ generate C as A-algebra. □

We prove that the concepts of p-basis and differential basis coincide for finite extensions of exponent one.

Proposition 2.53 ([44, Proposition 5.6])**.** *Let $A \subseteq C$ be a finite extension of exponent at most one and let $x_1, \dots, x_n \in C$. Then $\{x_1, \dots, x_n\}$ is a p-basis for C over A if and only if it is a differential basis.*

Proof. Let $\{x_1, \dots, x_n\}$ be a p-basis for C over A, so we have a presentation $C = A[X_1, \dots, X_n]/\langle X_1^p - x_1^p, \dots, X_n^p - x_n^p\rangle$. Then by [44, Proposition 4.19], we have that $\Omega_{C/A} = C dx_1 \oplus \cdots \oplus C dx_n$ and this implies that $\{dx_1, \dots, dx_n\}$ is a basis of $\Omega_{C/A}$ as C-module.

Conversely, assume that $\{dx_1, \dots, dx_n\}$ is a basis of $\Omega_{C/A}$ as C-module and let $C' := A[x_1, \dots, x_n]$. We claim that $\{x_1, \dots, x_n\}$ is a p-basis of C' over A. It is clear that the set of reduced monomials generate C' as an A-algebra, so we only have to check that they form a p-independent set over A. Let I be the ideal of polynomials $f \in A[X_1, \dots, X_n]$ with degree at most $p-1$ at each variable X_i such that $f(x_1, \dots, x_n) = 0 \in C$. By contradiction, we may assume that there is a $f \in I$ such that $f \neq 0$. Without loss of generality, we assume that X_1 appears in some

monomial in the expression of f. In addition, we can choose f so it contains the non-trivial monomial with lower degree in X_1 appearing on the polynomials from I. Note that we have a relation $\frac{\partial f}{\partial X_1}dx_1 + \cdots + \frac{\partial f}{\partial X_n}dx_n = 0 \in \Omega_{C/A}$. As $dx_1, \ldots, dx_n$ are linearly independent over C, we have that $\frac{\partial f}{\partial X_i} = 0$ for all i. In particular, $\frac{\partial f}{\partial X_1}$ is a non-trivial polynomial that belongs to I which contradicts the minimal property of f. Thus, $I = 0$ and the reduced monomials on $x_1, \ldots, x_n$ are linearly independent over A. So $\{x_1, \ldots, x_n\}$ is a p-basis for C' over A.

We make an abuse of notation and denote by d both the universal derivations of C' and C over A. Now, by the first implication, $dx_1, \ldots, dx_n$ generate $\Omega_{C'/A}$. Then the natural map $\Omega_{C'/A} \otimes_{C'} C \to \Omega_{C/A}$ is surjective. By Proposition 2.14, we have an exact sequence $\Omega_{C'/A} \otimes_{C'} C \to \Omega_{C/A} \to \Omega_{C/C'} \to 0$, so $\Omega_{C/C'} = 0$. Finally, since $C^p \subseteq C'$, we can apply Lemma 2.51 to conclude that $C = C'$. This completes the proof of the converse, since $\{x_1, \ldots, x_n\}$ is thus a p-basis for C over A. □

We can combine Lemma 2.52 and Proposition 2.53 to obtain a criteria for the existence of p-basis for finite extensions of local rings with exponent one.

Corollary 2.54. *Let $A \subseteq C$ be an exponent at most one finite extension of local rings. Then C has a p-basis over A if and only if $\Omega_{C/A}$ is a flat C-module. In this case, any minimal generating set $x_1, \ldots, x_n$ of C as an A-algebra is a p-basis.*

Proof. If $\{x_1, \ldots, x_n\}$ is a p-basis for C over A, then $\{x_1, \ldots, x_n\}$ is a differential basis by Proposition 2.53. Thus, $\Omega_{C/A}$ is a free C-module with basis $\{dx_1, \ldots, dx_n\}$. In particular, $\Omega_{C/A}$ is a flat C-module.

Conversely, assume that $\Omega_{C/A}$ is a flat C-module. Since $A \subseteq C$ is finite, $\Omega_{C/A}$ is a finite C-module by Proposition 2.16. Since C is local, Corollary A.37 implies that $\Omega_{C/A}$ is free as C-module. Then, by Proposition 2.53, we only need to prove that if $x_1, \ldots, x_n$ is a minimal generating set for C as A-algebra, then it is a differential basis. Now, by Lemma 2.52, $dx_1, \ldots, dx_n$ is a minimal generating set for $\Omega_{C/A}$. By Proposition A.36, we conclude that it has to be a basis. □

Finally, using the previous results, we obtain a characterization of Galois extensions in terms of the module of Kähler differentials.

Proposition 2.55. *Let $A \subseteq C$ be a finite ring extension of exponent at most one. Then the following conditions are equivalent:*

(1) $A \subseteq C$ is a Galois extension.

(2) C is an A-module of finite presentation and $\Omega_{C/A}$ is a flat C-module.

(3) $\Omega_{C/A}$ is a projective C-module.

(4) There exist $f_1, \ldots, f_r \in A$ generating the unit ideal such that C_{f_i} has a p-basis over A_{f_i}.

Proof. Let $A \subseteq C$ be a Galois extension. In particular, C has finite presentation as A-module (Remark 2.43). Note that $\Omega_{C/A}$ is a flat C-module if and only if $(\Omega_{C/A})_{\mathfrak{p}}$ is a flat $C_{\mathfrak{p}}$-module for every prime ideal $\mathfrak{p} \subset A$. By Proposition 2.17, we have an isomorphism $(\Omega_{C/A})_{\mathfrak{p}} \simeq \Omega_{C_{\mathfrak{p}}/A_{\mathfrak{p}}}$. Since $C_{\mathfrak{p}}$ has a p-basis over $A_{\mathfrak{p}}$, it follows by Corollary 2.54 that $\Omega_{C_{\mathfrak{p}}/A_{\mathfrak{p}}}$ is flat and this completes the implication (1)⇒(2).

Recall that any flat module of finite presentation is projective by Proposition 1.7. Then the implication (2)⇒(3) follows from the fact that if C has finite presentation as A-module, then $\Omega_{C/A}$ is a C-module of finite presentation (see Proposition 2.16.(2)).

We assume now that $\Omega_{C/A}$ is a projective C-module. The implication (3)⇒(4) follows if we show that given a prime ideal $\mathfrak{p} \subset A$, there is $h \in A \setminus \mathfrak{p}$ such that C_h has a p-basis over A_h. Since $A \subseteq C$ is finite, $\Omega_{C/A}$ is finitely generated as C-module by Proposition 2.16. Then $\Omega_{C/A}$ is locally free of finite rank by Proposition 1.7. Since $\mathrm{Spec}(A)$ and $\mathrm{Spec}(C)$ are homeomorphic (see Remark 2.2), there is $f \in A \setminus \mathfrak{p}$ such that Ω_{C_f/A_f} is a finite free C_f-module, say of rank n. We can choose $x_1, \ldots, x_n \in C$ such that, when they are viewed as elements of $C_{\mathfrak{p}}$, $dx_1, \ldots, dx_n$ is a minimal generating set for $\Omega_{C_{\mathfrak{p}}/A_{\mathfrak{p}}}$ as $C_{\mathfrak{p}}$-module. Then there is $g \in A \setminus \mathfrak{p}$ such that $\Omega_{C_{fg}/A_{fg}}$ is generated by $dx_1, \ldots, dx_n$, viewing $x_1, \ldots, x_n$ as elements in C_{fg}. By Proposition 2.17 and Proposition A.32, $\Omega_{C_{fg}/A_{fg}}$ is a free C_{fg}-module of rank n. Thus, $dx_1, \ldots, dx_n$ has to be a basis. We conclude that $x_1, \ldots, x_n$ is a p-basis for C_{fg} over A_{fg} by Proposition 2.53.

If $A \subseteq C$ satisfies condition (4), then C is a finite locally free A-module. Hence, C is projective by Proposition 1.7. Given a prime ideal $\mathfrak{p} \subset A$, we can choose f_i among the generators of the unit ideal such that $f_i \in A \setminus \mathfrak{p}$. Then the p-basis for C_{f_i} over A_{f_i} induces a p-basis for $C_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$ via the base change $A_{f_i} \to A_{\mathfrak{p}}$ (Lemma 2.25.(2)). Then $A \subset C$ is a Galois extension and this completes the proof of (4)⇒(1). □

2.2.3. Galois extensions and derivations

In this subsection, we explore the connection between Galois rings extensions of exponent one and derivations. We recover some ideas from the work of S. Yuan ([68]) and include the new perspective given in [11, §3.3] in collaboration with D. Sulca. We first study how derivations and p-basis are related.

2.56. *Derivations associated to a p-basis.* Let $A \subseteq C$ be a ring extension that admits a p-basis $\{x_1, \ldots, x_n\}$. We denote $\mathbf{x}^{\alpha} := x_1^{\alpha_1} \cdot \cdots \cdot x_n^{\alpha_n}$, for each $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$, and

$$\mathcal{A} := \{\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n : \ 0 \leq \alpha_i < p\}.$$

Then the set of reduced monomials $\{\mathbf{x}^{\alpha} : \ \alpha \in \mathcal{A}\}$ is a basis for C over A. For each $i \in \{1, \ldots, n\}$, we denote by $\mathbf{e}_i$ the n-tuple such that $(\mathbf{e}_i)_j = \delta_{ij}$. Then for each i there is an A-linear map $\partial_i \colon C \to C$ such that

$$\partial_i(\mathbf{x}^{\alpha}) = \begin{cases} \alpha_i \cdot \mathbf{x}^{\alpha - \mathbf{e}_i} & \text{if } \alpha_i \neq 0 \\ 0 & \text{if } \alpha_i = 0. \end{cases}$$

Indeed, $\partial_1, \ldots, \partial_n$ are A-derivations, which we call *partial derivatives associated to the p-basis* $\{x_1, \ldots, x_n\}$.

Proposition 2.57. *Let $A \subseteq C$ be a ring extension with p-basis $\{x_1, \ldots, x_n\}$. Then $\mathrm{Der}_A(C)$ is a free C-module with basis given by the partial derivatives $\{\partial_1, \ldots, \partial_n\}$. Moreover,*

$$A = \ker(\mathrm{Der}_A(C)) := \{x \in C : D(x) = 0,\ \forall D \in \mathrm{Der}_A(C)\}.$$

Proof. Note that any A-derivation $D\colon C \to C$ can be written as a C-linear combination of the partial derivatives as follows

$$D = \partial(x_1)\partial_1 + \cdots + \partial(x_n)\partial_n.$$

Thus, $\{\partial_1, \ldots, \partial_n\}$ is a set of generators for $\mathrm{Der}_A(C)$ as C-module. We check that it is linearly independent over C. Let $c_1\partial_1 + \ldots c_n\partial_n = 0$ be a C-linear relation. Then, for each $i = 1, \ldots, n$, we have

$$c_i = (c_1\partial_1 + \ldots c_n\partial_n)(x_i) = 0\,.$$

Hence, $\{\partial_1, \ldots, \partial_n\}$ is a basis for $\mathrm{Der}_A(C)$ as C-module. This implies that $\ker(\mathrm{Der}_A(C)) = \cap_{i=1}^n \ker(\partial_i)$. Therefore, by evaluating the derivations ∂_i at the reduced monomials, it follows that $\cap_{i=1}^n \ker(\partial_i) = A$. □

Moreover, for a ring extension $A \subseteq C$ with p-basis, the partial derivatives associated to the p-basis and the elements in C generate $\mathrm{End}_A(C)$ as an A-algebra. In order to prove it, we introduce the Taylor operators associated to the p-basis of the ring extension.

2.58. *Taylor operators associated to a p-basis.* Let $A \subseteq C$ be a ring extension with p-basis $\{x_1, \ldots, x_n\}$ as in (2.56). For each $\beta \in \mathcal{A}$, we define an A-linear map $\partial_\beta\colon C \to C$ given by

$$\partial_\beta(\mathbf{x}^\alpha) := \binom{\alpha}{\beta}\mathbf{x}^{\alpha-\beta} \quad \text{for each } \alpha \in \mathcal{A},$$

where the binomial coefficient is defined as

$$\binom{\alpha}{\beta} := \prod_{i=1}^n \binom{\alpha_i}{\beta_i}.$$

We call $\{\delta_\beta : \beta \in \mathcal{A}\}$ the *Taylor operators associated to the p-basis* $\{x_1, \ldots, x_n\}$. It can be shown that each δ_β is related to the partial derivatives as follows

$$\partial_\beta = \frac{1}{\beta!}\partial_1^{\beta_1} \circ \cdots \circ \partial_n^{\beta_n}, \qquad \text{where } \beta! := \prod_{i=1}^n \beta_i!.$$

Proposition 2.59. *Let $A \subseteq C$ be a ring extension with p-basis $\{x_1, \ldots, x_n\}$. Then $\mathrm{End}_A(C)$ is a free C-module with basis given by the Taylor operators $\{\partial_\beta : \beta \in \mathcal{A}\}$. Moreover, $\mathrm{End}_A(C) = C[\mathrm{Der}_A(C)]$.*

Proof. For each $\alpha \in \mathcal{A}$, we define an A-linear map $\phi_\alpha \colon C \to A$ as

$$\phi_\alpha(\mathbf{x}^\beta) = \begin{cases} 1 & \text{if } \alpha = \beta \\ 0 & \text{if } \alpha \neq \beta\,. \end{cases}$$

Then we can express any $\varphi \in \mathrm{End}_A(C)$ as the C-linear combination

$$\varphi = \sum_{\alpha \in \mathcal{A}} \varphi(\mathbf{x}^\alpha)\, \phi_\alpha\,.$$

Observe that $\phi_\alpha = \sum_{\beta \in \mathcal{A}} \phi_\alpha(\mathbf{x}^\beta) \cdot \partial_\beta$. Thus, every $\varphi \in \mathrm{End}_A(C)$ can be written as a C-linear combination of the Taylor operators $\{\partial_\beta : \beta \in \mathcal{A}\}$. In order to show that $\{\partial_\beta : \beta \in \mathcal{A}\}$ is a basis for $\mathrm{End}_A(C)$, we have to check that it is a linearly independent subset over C. Let $\sum_{\beta \in \mathcal{A}} c_\beta \cdot \partial_\beta = 0$ be a C-linear relation. We evaluate this relation at $\mathbf{x}^\alpha$ for each $\alpha \in \mathcal{A}$, so we have

$$0 = \sum_{\beta \in \mathcal{A}} c_\beta \cdot \partial_\beta(\mathbf{x}^\alpha) = \sum_{\beta \in \mathcal{A}} c_\beta \cdot \binom{\alpha}{\beta} \mathbf{x}^{\alpha - \beta}.$$

Note that for $\beta \in \mathcal{A}$ such that $\alpha_i < \beta_i$ for some $i \in \{1, \ldots, n\}$, the corresponding term in the above sum is zero, and that for $\beta = \alpha$ the corresponding term is c_α. Let $|\alpha| = \alpha_1 + \cdots + \alpha_n$. In particular, for $|\alpha| = 0$, the above relation reads as $c_\alpha = 0$. Then proceeding inductively on $|\alpha|$ for $\alpha \in \mathcal{A}$, we deduce that $c_\beta = 0$ for all $\beta \in \mathcal{A}$.

Finally, it is clear that $C[\mathrm{Der}_A(C)] \subseteq \mathrm{End}_A(C)$ and the reverse inclusion is a direct consequence of the above argument, since $\{\partial_\beta : \beta \in \mathcal{A}\}$ is a basis for $\mathrm{End}_A(C)$ as C-module and $\partial_\beta = \frac{1}{\beta!} \partial_1^{\beta_1} \circ \cdots \circ \partial_n^{\beta_n}$. □

Remark 2.60. If $A \subseteq C$ is a ring extension with p-basis, then $\mathrm{Der}_A(C)$ is a C-direct summand of $\mathrm{End}_A(C)$. In fact, by Proposition 2.57, the partial derivatives associated to the p-basis form a basis for $\mathrm{Der}_A(C)$ as C-module. Since these derivations are also Taylor operators, they are part of a basis for $\mathrm{End}_A(C)$ as C-module by Proposition 2.59.

We use the above results on the derivations of a ring extension with p-basis to deduce some properties for Galois ring extensions of exponent one.

Lemma 2.61. *Let $A \subseteq C$ be a Galois extension of exponent one. Then $\mathrm{Der}_A(C)$ is a finitely generated and projective C-module.*

Proof. By Proposition 2.55, there exist $f_1, \ldots, f_r \in A$ generating the unit ideal such that C_{f_i} has a p-basis over A_{f_i}. Given a prime ideal $\mathfrak{p} \subset A$, we have $f_i \in A \setminus \mathfrak{p}$ for some $i \in \{1, \ldots, n\}$. Note that $\mathrm{Der}_{A_{f_i}}(C_{f_i})$ is a finite free C_{f_i}-module by Proposition 2.57. Recall that C is an A-module of finite presentation as we noted in Remark 2.43. Hence, $(\mathrm{Der}_A(C))_{f_i} \simeq \mathrm{Der}_{A_{f_i}}(C_{f_i})$ by Corollary 2.18. Therefore, $\mathrm{Der}_A(C)$ is a locally free C-module of finite rank. Finally, we conclude that $\mathrm{Der}_A(C)$ is finitely generated and projective as C-module by Proposition 1.7. □

Proposition 2.62 ([68, Theorem 9])**.** *Let $A \subseteq C$ be a Galois extension of exponent one. Then*

(1) $\mathrm{End}_A(C) = C[\mathrm{Der}_A(C)]$.

(2) $\mathrm{Der}_A(C) \subseteq \mathrm{End}_A(C)$ *is a direct summand as* C*-module.*

In addition, $A = \ker(\mathrm{Der}_A(C)) = \{x \in C : D(x) = 0,\ \forall D \in \mathrm{Der}_A(C)\}$.

Proof. By hypothesis, $C_\mathfrak{p}$ has a p-basis over $A_\mathfrak{p}$ for every prime ideal $\mathfrak{p} \subset A$. Thus, by Proposition 2.59, the extension $A_\mathfrak{p} \subset C_\mathfrak{p}$ satisfies the next conditions:

(1') $\mathrm{End}_{A_\mathfrak{p}}(C_\mathfrak{p}) = C_\mathfrak{p}[\mathrm{Der}_{A_\mathfrak{p}}(C_\mathfrak{p})]$.

(2') $\mathrm{Der}_{A_\mathfrak{p}}(C_\mathfrak{p}) \subseteq \mathrm{End}_{A_\mathfrak{p}}(C_\mathfrak{p})$ is a direct summand as $C_\mathfrak{p}$-module.

Recall that $A \subseteq C$ is a finite ring extension such that C is a projective A-module. In particular, C has finite presentation as A-module by Proposition 1.7. Hence, $\mathrm{End}_A(C)$ and $\mathrm{Der}_A(C)$ behave well under localization by Corollary 1.25 and Corollary 2.18. Therefore, condition (1') implies that $(\mathrm{End}_A(C))_\mathfrak{p} \simeq (C[\mathrm{Der}_A(C)])_\mathfrak{p}$ for every prime ideal $\mathfrak{p} \subset A$ and the equality in (1) holds by Lemma A.9.

We prove now that $A \subseteq C$ satisfies condition (2). By Proposition 1.23, $\mathrm{End}_A(C)$ is a finite projective C-module. In particular, it is a C-module of finite presentation by Proposition 1.7. Note that $\mathrm{Der}_A(C)$ is a finitely generated C-module by Lemma 2.61. Then it follows by Proposition A.25 that the quotient $\mathrm{End}_A(C)/\mathrm{Der}_A(C)$ has finite presentation as C-module. Finally, by Lemma A.30, $\mathrm{Der}_A(C)$ is a C-direct summand of $\mathrm{End}_A(C)$ if and only if $\mathrm{Der}_{A_\mathfrak{p}}(C_\mathfrak{p})$ is a $C_\mathfrak{p}$-direct summand of $\mathrm{End}_{A_\mathfrak{p}}(C_\mathfrak{p})$ for all $\mathfrak{p} \subset A$. Since this is condition (2'), the result holds.

Finally, the last affirmation is true if and only if it holds when we localize at each prime ideal $\mathfrak{p} \subset A$, by Lemma A.9. This result implies also that $(\ker(\mathrm{Der}_A(C)))_\mathfrak{p} \simeq \ker((\mathrm{Der}_A(C))_\mathfrak{p})$. The later module is isomorphic to $\ker(\mathrm{Der}_{A_\mathfrak{p}}(C_\mathfrak{p}))$ by Corollary 2.18. Since $A_\mathfrak{p} = \ker(\mathrm{Der}_{A_\mathfrak{p}}(C_\mathfrak{p}))$ by Proposition 2.57, the proof is complete. □

In fact, the two conditions in the above proposition characterize Galois extensions among finite projective ring extensions of exponent one. In [68], S. Yuan proved that condition (1) is sufficient for such an extension to be Galois. We include here a proof for this fact.

Proposition 2.63 ([68, Theorem 10])**.** *Let* $A \subseteq C$ *be a finite ring extension of exponent at most one such that* C *is projective as* A*-module. If* $\mathrm{End}_A(C) = C[\mathrm{Der}_A(C)]$*, then* $A \subseteq C$ *is a Galois extension.*

Proof. By Corollary 2.48, the extension $A \subseteq C$ is Galois if and only if $C_\mathfrak{p}/\mathfrak{p}C_\mathfrak{p}$ is differentiably simple for every prime ideal $\mathfrak{p} \subset A$. So we prove this equivalent condition.

Let $\kappa(\mathfrak{p}) := A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ and $\bar{C}_\mathfrak{p} := C_\mathfrak{p}/\mathfrak{p}C_\mathfrak{p}$. We begin with some observations. Using Corollary 1.25 and Corollary 2.18, the assumptions imply that $\mathrm{End}_{A_\mathfrak{p}}(C_\mathfrak{p}) = C_\mathfrak{p}[\mathrm{Der}_{A_\mathfrak{p}}(C_\mathfrak{p})]$. In addition, $\mathrm{End}_{A_\mathfrak{p}}(C_\mathfrak{p}) \otimes_{A_\mathfrak{p}} \kappa(\mathfrak{p}) \simeq \mathrm{End}_{\kappa(\mathfrak{p})}(\bar{C}_\mathfrak{p})$ by Lemma 1.24. We denote by H the image of $\mathrm{Der}_{A_\mathfrak{p}}(C_\mathfrak{p}) \otimes_{A_\mathfrak{p}} \kappa(\mathfrak{p})$ in $\mathrm{End}_{\kappa(\mathfrak{p})}(\bar{C}_\mathfrak{p})$. Note that H is a module of derivations of $\bar{C}_\mathfrak{p}$ and that $\mathrm{End}_{\kappa(\mathfrak{p})}(\bar{C}_\mathfrak{p}) = \bar{C}_\mathfrak{p}[H]$.

Let I be a proper differential ideal of $\bar{C}_{\mathfrak{p}}$. Then $D(I) \subseteq I$ for each derivation $D \in H$ and $\varphi(I) \subseteq I$ for any $\varphi \in \mathrm{End}_{\kappa(\mathfrak{p})}(\bar{C}_{\mathfrak{p}})$. Thus, I can be considered as a proper (left) $\mathrm{End}_{\kappa(\mathfrak{p})}(\bar{C}_{\mathfrak{p}})$-submodule of $\bar{C}_{\mathfrak{p}}$. We claim that $\bar{C}_{\mathfrak{p}}$ has no non-trivial proper submodules when it is considered as an $\mathrm{End}_{\kappa(\mathfrak{p})}(\bar{C}_{\mathfrak{p}})$-module. In fact, for any non-zero $x \in \bar{C}_{\mathfrak{p}}$ we can find $\varphi_\lambda \in \mathrm{End}_{\kappa(\mathfrak{p})}(\bar{C}_{\mathfrak{p}})$ such that $\{\varphi_\lambda(x) : \lambda \in \Lambda\}$ form a basis for $\bar{C}_{\mathfrak{p}}$ as $\kappa(\mathfrak{p})$-vector space, so any $\mathrm{End}_{\kappa(\mathfrak{p})}(\bar{C}_{\mathfrak{p}})$-submodule containing a non-zero element is equal to $\bar{C}_{\mathfrak{p}}$. Therefore, since I is a proper submodule, we conclude that $I = 0$ and this completes the proof. □

In [11], we demonstrate that condition (2) in Proposition 2.62 is also sufficient for a finite projective ring extension of exponent one to be Galois. We will recall the proof of this fact in Proposition 2.67. With this aim, we include here the technical lemmas used to prove it. We note that the proof of the next lemma is contained in the last paragraph of the proof of [68, Theorem 12], which in turn follows the lines of G. Hochschild's proof of [32, Theorem 1].

Lemma 2.64. *Let C be a ring and let $x_1, \ldots, x_n \in C$. If there exist derivations $D_1, \ldots, D_n$ of C such that*

$$D_i(x_j) = \delta_{ij}, \quad [D_i, D_j] = 0, \quad D_i^p = 0, \quad \forall i, j \in \{1, \ldots, n\},$$

then $\{x_1, \ldots, x_n\}$ is a p-basis for C over $A := \cap_{i=1}^n \ker(D_i)$ and $\{D_1, \ldots, D_n\}$ are the associated partial derivatives. In particular, $\{D_1, \ldots, D_n\}$ is a basis for the C-module $\mathrm{Der}_A(C)$.

Proof. For $\beta = (\beta_1, \ldots, \beta) \in \mathbb{N}_0^n$, we set $D_\beta := D_1^{\beta_1} \circ \cdots \circ D_n^{\beta_n}$. It is easy to show that $\frac{1}{\beta!} D_\beta(\mathbf{x}^\alpha) = \binom{\alpha}{\beta} \mathbf{x}^{\alpha-\beta}$ for all $\alpha, \beta \in \mathcal{A}$, and that $D_\beta = 0$ for $\beta \notin \mathcal{A}$ since $D_i^p = 0$ for all i. We claim that $\{x_1, \ldots, x_n\}$ is a p-basis for $C' := A[x_1, \ldots, x_n]$ over A. In fact, we only have to check that the reduced monomials $\{\mathbf{x}^\alpha : \alpha \in \mathcal{A}\}$ are linearly independent over A. Given an A-linear relation $\sum_{\alpha \in \mathcal{A}} a_\alpha \mathbf{x}^\alpha = 0$, it is easy to deduce that $a_\alpha = 0$ by evaluating each D_β on the relation. Thus, it remains to show that $C' = C$.

Let $c \in C$ be a non-zero element. We have to prove that $c' \in C$. For each $\alpha \in \mathbb{N}_0^n$, set $|\alpha| := \alpha_1 + \cdots + \alpha_n$. We define $d(c) := \max\{|\alpha| : \alpha \in \mathcal{A},\ D_\alpha(c) \neq 0\}$, which exists because $\mathcal{A}$ is a finite set and $D_0(c) = c \neq 0$. We proceed by induction on $d(c)$. If $d(c) = 0$, then $D_i(c) = 0$ for all i. Since $A = \cap_{i=1}^n \ker(D_i)$, this implies that $c \in A \subset C'$. Now, suppose that $d(c) = k > 0$. For each $\alpha \in \mathcal{A}$ such that $|\alpha| = k$, we set $a_\alpha := \frac{1}{\alpha!} D_\alpha(c)$. Since $[D_i, D_j] = 0$ for all $i, j \in \{1, \ldots, n\}$, we have that $D_i(a_\alpha) = \frac{1}{\alpha!} D_{\alpha + \mathbf{e}_i}(c)$, for $i = 1, \ldots, n$. Note that $D_i(a_\alpha) = 0$, since $D_{\alpha+\mathbf{e}_i} = 0$ if $\alpha + \mathbf{e}_i \notin \mathcal{A}$, and $D_{\alpha+\mathbf{e}_i}(c)$ is also zero if $\alpha + \mathbf{e}_i \in \mathcal{A}$ by the maximal property of k. Therefore, by the definition of A, we have that $a_\alpha \in A$. Let $c' := c - \sum_{|\alpha|=k} a_\alpha \mathbf{x}^\alpha$. If $c' = 0$, then $c = \sum_{|\alpha|=k} a_\alpha \mathbf{x}^\alpha \in C'$. In other case, $d(c') < k$ and $c' \in C'$ by the inductive hypothesis, so $c \in C'$. Thus, $C = C'$, as we wanted, and $\{x_1, \ldots, x_n\}$ is a p-basis for C over A. In addition, observe that the derivations $D_1, \ldots, D_n$ coincide with the associated partial derivatives, so they are a basis for $\mathrm{Der}_A(C)$ as C-module (see Proposition 2.57). □

Lemma 2.65. *Let $A \subseteq C$ be a finite ring extension of finite exponent such that C is projective as A-module. If $\mathrm{Der}_A(C) = 0$, then $A = C$.*

Proof. Let $J \subseteq C \otimes_A C$ be the kernel of the multiplication map as in (2.12). Since C is a projective A-module, the exact sequence

$$0 \to J \to C \otimes_A C \to C \to 0$$

splits by Proposition 1.2. So $C \otimes_A C = C \oplus J$. By Remark 1.9, $C \otimes_A C$ as finite and projective as (left) C-module. Since J is a direct summand of $C \otimes_A C$, it follows by Proposition 1.2 that J is also projective as a C-module. In addition, note that J is finitely generated by Proposition A.25.(3).

We prove by induction that $\mathrm{Hom}_C(J^k/J^{k+1}, C) = 0$ for all $k \geq 1$. For $k = 1$, we have $\mathrm{Hom}_C(J/J^2, C) = \mathrm{Hom}_C(\Omega_{C/A}, C) = \mathrm{Der}_A(C) = 0$, as we noted in (2.19). Let $k > 1$ and suppose that $\mathrm{Hom}_C(J^{k-1}/J^k, C) = 0$. We have to prove that $\mathrm{Hom}_C(J^k/J^{k+1}, C) = 0$. We proceed by contradiction and assume that there is a non-zero $\varphi \in \mathrm{Hom}_C(J^k/J^{k+1}, C)$. Then there are $x \in J$ and $y \in J^{k-1}$, so $xy \in J^k$, such that $\varphi(xy + J^{k+1}) \neq 0$. But then the map $\psi\colon J^{k-1}/J^k \to C$ defined by $\psi(u + J^k) := \varphi(xu + J^{k+1})$ is a non-zero C-module homomorphism, contradicting the inductive hypothesis. Thus, it must be $\mathrm{Hom}_C(J^k/J^{k+1}, C) = 0$.

We use the above fact to prove that $J = 0$. For each $k \geq 1$, we have an exact sequence

$$0 \to J^k/J^{k+1} \to J/J^{k+1} \to J/J^k \to 0,$$

that induce the left exact sequence of C-modules

$$0 \to \mathrm{Hom}_C(J/J^k, C) \to \mathrm{Hom}_C(J/J^{k+1}, C) \to \mathrm{Hom}_C(J^k/J^{k+1}, C).$$

Since $\mathrm{Hom}_C(J^k/J^{k+1}, C) = 0$, the above left exact sequence induces an isomorphism $\mathrm{Hom}_C(J/J^{k+1}, C) \simeq \mathrm{Hom}_C(J/J^k, C)$ for all $k \geq 1$. We claim that J is a nilpotent ideal, i.e., there exists $n \geq 1$ such that $J^{n+1} = 0$. In fact, $A \subseteq C$ has finite exponent, say e, so $x^{p^e} \in A$ for all $x \in C$. Since J is generated by the elements of the form $1 \otimes x - x \otimes 1$ with $x \in C$, we have

$$(1 \otimes x - 1 \otimes x)^{p^e} = 1 \otimes x^{p^e} - x^{p^e} \otimes 1 = x^{p^e} \cdot (1 \otimes 1) - x^{p^e} \otimes 1 = 0,$$

and $J^{n+1} = 0$ for $n = p^e - 1$. Then $J \simeq J/J^{n+1}$ and $\mathrm{Hom}_C(J, C) = \mathrm{Hom}_C(J/J^{n+1}, C)$. Recall that this is equal to $\mathrm{Hom}_C(J/J^n, C) = \cdots = \mathrm{Hom}_C(J/J^2, C) = 0$ as we have proved before. Therefore, we have that $J^* := \mathrm{Hom}_C(J, C) = 0$. Since J is a finite projective C-module, we have by Proposition 1.10 that $J \simeq J^{**}$. Hence, we conclude that $J = 0$.

Finally, since $C \otimes_A C = C \oplus J$ and $J = 0$, we have that $C \otimes_A C = C$. By Remark 1.16, $A \subset C$ is faithfully flat. Thus, we deduce that $C = A$, as we wanted to prove. □

Lemma 2.66. *Let $A \subseteq C$ be a finite ring extension of exponent at most one such that C is projective as A-module. Let B be an intermediate subring, $A \subseteq B \subset C$, such that C has a p-basis over B. If $\mathrm{Der}_A(C) = \mathrm{Der}_B(C)$, then $A = B$.*

Proof. The fact that C has a p-basis over B implies that C is a finite free B-module. Then, by Lemma 1.17, B is a finitely generated projective A-module. Let $\{x_1, \ldots, x_n\}$

be a p-basis for C over B and denote $a_i := x_i^p \in A$. Then we have

$$C = \frac{B[X_1, \ldots, X_n]}{\langle X_1^p - a_1, \ldots, X_n^p - a_n \rangle} = B \otimes_A \frac{A[X_1, \ldots, X_n]}{\langle X_1^p - a_1, \ldots, X_n^p - a_n \rangle}.$$

By contradiction, assume that $A \neq B$. Then, by Lemma 2.65, there is a non-zero derivation $D \in \mathrm{Der}_A(B)$. By the above equality, there is a non-zero derivation $\tilde{D} \in \mathrm{Der}_A(C)$ such that $\tilde{D}|_B = D$. Since $\tilde{D}(B) \neq 0$, $\tilde{D} \notin \mathrm{Der}_B(C)$. But this contradicts the hypothesis $\mathrm{Der}_A(C) = \mathrm{Der}_B(C)$. Thus $A = B$. □

Finally, we obtain the new criteria for a finite projective ring extension of exponent one to be Galois.

Proposition 2.67. *Let $A \subseteq C$ be a finite extension of exponent at most one such that C is a projective A-module. If $\mathrm{Der}_A(C)$ is C-module direct summand of $\mathrm{End}_A(C)$, then $A \subseteq C$ is a Galois extension.*

Proof. By Corollary 1.25 and Corollary 2.18, $\mathrm{End}_A(C)$ and $\mathrm{Der}_A(C)$ behave well under localization. Hence, we may assume that A is a local ring. Since $\mathrm{Spec}(A)$ and $\mathrm{Spec}(C)$ are homeomorphic (see Remark 2.2), C is also local.

Taking $H = \mathrm{Der}_A(C)$ in Lemma 1.27, we obtain elements $x_1, \ldots, x_n \in C$ and a basis $D_1, \ldots, D_n$ for $\mathrm{Der}_A(C)$ as C-module such that $D_i(x_j) = \delta_{ij}$ for all $i, j \in \{1, \ldots, n\}$. We show that they satisfy the conditions in Lemma 2.64, i.e., that $[D_i, D_j] = D_i^p = 0$ for all $i, j \in \{1, \ldots, n\}$. Since $\mathrm{Der}_A(C)$ is a restricted Lie algebra, $[D_i, D_j], D_i^p \in \mathrm{Der}_A(C)$ for all $1 \leq i, j \leq n$. Then we have

$$[D_i, D_j] = \sum_{k=1}^{n} c_{ij}^{(k)} D_k, \quad \text{and} \quad D_i^p = \sum_{k=1}^{n} c_i^{(k)} D_k \quad \text{for some } c_{ij}^{(k)}, c_i^{(k)} \in C.$$

Observe that $c_{ij}^{(k)} = [D_i, D_j](x_k) = 0$ and $c_i^{(k)} = D_i^p(x_k) = 0$, for $k = 1, \ldots, n$. Thus, $[D_i, D_j] = D_i^p = 0$ for all $i, j \in \{1, \ldots, n\}$, as we wanted to show. Then, by Lemma 2.64, $\{x_1, \ldots, x_n\}$ is a p-basis for C over $B := \cap_{i=1}^n \ker(D_i)$, and $D_1, \ldots, D_n$ is a basis for $\mathrm{Der}_B(C)$ as C-module. In particular, $\mathrm{Der}_A(C) = \mathrm{Der}_B(C)$. Finally, we conclude that $B = A$ by Lemma 2.66. Thus C has a p-basis over A. This implies that $A \subseteq C$ is Galois by Lemma 2.45.(1). □

2.2.4. Summary of characterizations of Galois extensions

In this final subsection, we collect the characterizations of Galois ring extensions of exponent one derived from the results previously exposed. We recall first the notion of purely inseparable ring extension of exponent one and we show that it coincides with the notion of Galois extension.

Definition 2.68. A finite ring extension $A \subseteq C$ is a *purely inseparable extension of exponent one* if the following conditions hold:

(i) $A \subseteq C$ has exponent at most one, i.e, $C^p \subseteq A$,

(ii) C is a projective A-module, and

(iii) for every prime ideal $\mathfrak{p} \subset A$, there exists a faithfully flat homomorphism $A_{\mathfrak{p}} \to A'$ such $C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A'$ has a splitting p-basis over A'.

Any Galois extension is purely inseparable, by Corollary 2.28.(2) and the fact that it is faithfully flat (see Remark 1.16). The converse is also true by the following lemma on faithfully flat descent of p-basis.

Lemma 2.69. *Let $A \subseteq C$ be an exponent at most one finite extension of local rings. If there is a faithfully flat homomorphism $A \to A'$ such that $C \otimes_A A'$ has p-basis over A', then C has a p-basis over A.*

Proof. Let $C' := C \otimes_A A'$. Since $A \to A'$ is faithfully flat, the base change $C \to C'$ is also faithfully flat (Proposition A.16). Since C' has a p-basis over A', the C'-module $\Omega_{C'/A'}$ is flat by Proposition 2.53. Recall that $\Omega_{C'/A'} \simeq \Omega_{C/A} \otimes_C C'$ by Proposition 2.17. Then, $\Omega_{C/A}$ is a flat C-module by faithfully flat descent (Proposition A.15.(2)). Thus, we conclude that $A \subset C$ has a p-basis by Corollary 2.54. □

The above lemma implies also that Galois extensions of rings are preserved under faithfully flat descent.

Proposition 2.70. *Let $A \subseteq C$ be a finite ring extension. If $A \to A'$ is a faithfully flat homomorphism of rings such that $A' \subseteq C \otimes_A A'$ is Galois, then $A \subseteq C$ is also Galois.*

Proof. Let $C' := C \otimes_A A'$. Since $A' \subseteq C'$ is Galois, it is a finite ring extension such that C' is projective as A'-module. Since the map $A \to A'$ is faithfully flat, we have that $A \subseteq C$ is also a finite projective extension of exponent one (see Proposition 1.4.(2) and Lemma 2.9). Finally, we show that $C_{\mathfrak{p}}$ has a p-basis over $A_{\mathfrak{p}}$ for each prime ideal $\mathfrak{p} \subset A$. Since $A \to A'$ is faithfully flat, the induced map on the spectra $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$ is surjective (Proposition A.19). Then for each prime ideal $\mathfrak{p} \subset A$, we can choose $\mathfrak{q} \subset A'$ such that $\mathfrak{q} \mapsto \mathfrak{p}$ in the above morphism. Note that $A_{\mathfrak{p}} \to A'_{\mathfrak{q}}$ is a flat local homomorphism between local rings, so it is faithfully flat (Corollary A.20). Since $A' \subseteq C'$ is Galois, the extension $A'_{\mathfrak{q}} \subseteq C'_{\mathfrak{q}}$ admits a p-basis. As $C'_{\mathfrak{q}} = C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A'_{\mathfrak{q}}$, we conclude that $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}}$ admits also a p-basis by Lemma 2.69. □

The next theorem summarizes the equivalences of the notion of Galois ring extension of exponent one that follow from the results exposed throughout the section.

Theorem 2.71. *Let $A \subseteq C$ be a finite ring extension of exponent at most one. Then the following conditions are equivalent:*

(1) $A \subseteq C$ is a purely inseparable extension.

(2) $A \subseteq C$ is a Galois extension.

(3) C *is a projective* A*-module and* $C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ *is differentiably simple for each prime ideal* $\mathfrak{p} \subset A$.

(4) $\Omega_{C/A}$ *is a projective* C*-module.*

(5) C *is a projective* A*-module and* $\mathrm{End}_A(C) = C[\mathrm{Der}_A(C)]$.

(6) C *is a projective* A*-module and* $\mathrm{Der}_A(C)$ *is a* C*-direct summand of* $\mathrm{End}_A(C)$.

Proof. The equivalence (1)⇔(2) is a consequence of the previous observations from this section. Recall that corollary 2.48 establishes equivalence (2)⇔(3). We have that (2)⇔(4) by Proposition 2.55. The implications (2)⇒(5) and (2)⇒(6) are a consequence of Proposition 2.62. While the converse implications (5)⇐(2) and (6)⇐(2) follow by Proposition 2.63 and Proposition 2.67 respectively. □

2.3. Towers of Galois extensions

This section is devoted to the study of Galois towers of rings from a geometric perspective. We begin with a review of some basic results on Galois towers of rings in Subsection 2.3.1. Then we include some preliminaries on affine group schemes in Subsection 2.3.2. In particular, we study the automorphism group scheme of an extension with splitting p-basis in Subsection 2.3.3. Finally, we introduce the *Yuan functor* to parametrize the subrings of a Galois extension that induce a Galois tower of fixed differential ranks, we show that it is representable by an scheme and we study some of its geometric properties in Subsection 2.3.4.

2.3.1. Basics on Galois towers of rings

In this subsection, we work in the setting of rings of prime characteristic p. We introduce Galois towers of rings and recall two important results concerning Galois extensions: the characterization from M. André for the intermediate subrings of a Galois extension that induce a Galois tower ([1]) and S. Yuan's correspondence between Galois towers and some restricted Lie subalgebras of the module of derivations ([68]).

Definition 2.72. A tower of rings $A \subseteq B \subseteq C$ is a *Galois tower* if the extensions $A \subseteq C$, $A \subseteq B$ and $B \subseteq C$ are Galois extensions of exponent one.

Towers of Galois extensions are well-understood. On the one hand, we have seen that the composition of two Galois extensions $A \subseteq B$ and $B \subseteq C$ induces a Galois tower $A \subseteq B \subseteq C$ when $A \subseteq C$ is a finite extension of exponent one (Lemma 2.45.(3)). On the other hand, S. Yuan proved in [68, Theorem 11] that any tower of rings $A \subseteq B \subseteq C$ such that C is Galois over both A and B is in fact a Galois tower. Moreover, given $A \subseteq C$ a Galois extension, M. André ([1]) proved that $A \subseteq B \subseteq C$ is a Galois tower if and only if C is projective as B-module, using homological methods. We give an alternative proof using the characterization of Galois extensions in terms of differentiably simple rings.

Proposition 2.73 ([1, Théorème 71]). *Let $A \subseteq C$ be a Galois extension of exponent one and let B be an intermediate subring, $A \subseteq B \subseteq C$. Then $B \subseteq C$ is Galois if and only if C is projective as B-module. In that case, $A \subseteq B$ is also Galois.*

Proof. We begin with some observations. Note first that both intermediate extensions $A \subseteq B$ and $B \subseteq C$ have exponent at most one. Since C is finitely generated as A-module, it is also finitely generated as B-module (Proposition A.27.(1)).

By definition, any Galois extension $B \subseteq C$ is such that C is projective as B-module. We prove the converse and assume that C is projective as B-module. Then B is a direct summand of C as B-module by Lemma 1.15. In particular, B is a direct summand of C as A-module. Since B is a direct summand of a finitely generated A-module, it is also finitely generated over A. Therefore, $A \subseteq B$ and $B \subseteq C$ are finite projective ring extensions of exponent one. By Corollary 2.48, the extensions are Galois if we prove that the fibers are differentiably simple. That is, we have to prove that for any prime ideals $\mathfrak{p} \subset A$ and $\mathfrak{q} \subset B$ with $\mathfrak{p} = A \cap \mathfrak{q}$, the rings $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ and $C_{\mathfrak{q}}/\mathfrak{q}C_{\mathfrak{q}}$ are differentiably simple.

Using the natural identifications $\mathrm{Spec}(A) \simeq \mathrm{Spec}(B) \simeq \mathrm{Spec}(C)$ (see Remark 2.2) and the equality $C_{\mathfrak{p}} = C_{\mathfrak{q}}$, we have $C_{\mathfrak{q}}/\mathfrak{q}C_{\mathfrak{q}} \simeq C_{\mathfrak{p}}/\mathfrak{q}C_{\mathfrak{p}}$. Since $A \subset C$ is Galois, we know that $C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ is differentiably simple by Corollary 2.48. Note that C is a flat B-module because C is finite projective over B (Proposition 1.7). So the map $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \to C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ is also flat as it is a base change of $B \to C$ (Proposition A.15). Observe that both rings $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ and $C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ are finite over the field $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$, so they are Noetherian (Proposition A.4). In brief, $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \to C_{\mathfrak{p}}/\mathfrak{p}C_{\mathfrak{p}}$ is a flat local homomorphism of Noetherian local rings. Since $\mathfrak{q}B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ is the maximal ideal of $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$, we conclude by Theorem 2.39 that $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ and $C_{\mathfrak{p}}/\mathfrak{q}C_{\mathfrak{p}}$ are differentiably simple, as we wanted. □

The motivation of S. Yuan to study Galois towers of rings was to develop a "Galois" correspondence extending the correspondence given by N. Jacobson for purely inseparable extensions of fields of exponent one. Namely, N. Jacobson stated a one-to-one correspondence for finite purely inseparable field extensions of exponent one between the subfields E of such an extension $K \subseteq L$ and the restricted Lie subalgebras of the module of derivations $\mathrm{Der}_K(L)$ ([36]). While, S. Yuan achieved the following correspondence for Galois extensions of rings of exponent one.

Theorem 2.74 (Yuan's correspondence, [68, Theorem 13]). *Let $A \subseteq C$ be a Galois extension of exponent one. There is a bijection between the following subset of rings*

$$\mathcal{G}_{C/A} := \left\{ B : \begin{array}{l} B \text{ is an intermediate subring } A \subseteq B \subseteq C \\ \text{and } C \text{ is a Galois extension of } B \end{array} \right\} \Bigg($$

and the following subset of restricted Lie subalgebras

$$\mathcal{RL}_{C/A} := \left\{ H : \begin{array}{l} H \text{ is a restricted Lie } A\text{-subalgebra of } \mathrm{Der}_A(C) \text{ and} \\ \text{a direct summand of } \mathrm{Der}_A(C) \text{ as } C\text{-module} \end{array} \right\} \Bigg($$

given by the following inverse maps

$$\begin{array}{ccc} \mathcal{G}_{C/A} & \to \mathcal{RL}_{C/A}, & \mathcal{RL}_{C/A} \to \mathcal{G}_{C/A} \\ B & \mapsto \mathrm{Der}_B(C) & H \mapsto \ker(H)\,, \end{array}$$

where $\ker(H) := \{x \in C : D(x) = 0,\ \forall D \in H\}$. *Moreover, for any subring* $B \in \mathcal{G}_{C/A}$, *the intermediate extension* $A \subset B$ *is Galois.*

Remark 2.75. Using the characterization of Galois towers given in Proposition 2.73, we have that

$$\mathcal{G}_{C/A} = \left\{ B : \begin{array}{l} B \text{ is an intermediate subring } A \subseteq B \subseteq C \\ \text{and } C \text{ is a } B\text{-projective module} \end{array} \right\} = \mathcal{P}_{C/A}$$

as in the extended version of Jacobson-Bourbaki correspondence (Theorem 1.30).

2.3.2. Preliminaries on affine group schemes

In this subsection, we return to the setting of rings in any characteristic and recall some generalities about affine group schemes. A more detailed introduction can be found in [18] for group schemes in general and in [48] for group schemes over a field. We introduce the automorphism group scheme (and some variants) of an arbitrary algebra (not necessarily commutative nor associative) that is finite and projective as a module over the base ring. The rings in this subsection are of any characteristic, not necessarily prime.

2.76. *Group schemes and Hopf algebras.* Let A be a ring. We denote by Alg_A, Groups and Sets the categories of A-algebras, groups and sets, respectively. A *group functor over* A is a covariant functor

$$\mathbf{G}\colon \mathrm{Alg}_A \to \mathrm{Groups}\,.$$

A group functor $\mathbf{G}$ is an *affine group scheme over* A if, in addition, the composition of $\mathbf{G}$ with the forgetful functor Groups $\to$ Sets is representable by an A-algebra. In other words, if there exists an A-algebra H and an element $\sigma \in \mathbf{G}(H)$, called *universal*, such that for any $A' \in \mathrm{Alg}_A$ there is a bijection

$$\begin{array}{rl} \mathrm{Hom}_A(H, A') \cong \mathbf{G}(A') & \text{(2.76.1)} \\ \varphi \mapsto \mathbf{G}(\varphi)(\sigma). & \end{array}$$

The group structure on $\mathbf{G}$ endows H with a structure of commutative Hopf algebra over A. It is called the *Hopf algebra* of $\mathbf{G}$ (see [48, Definition 3.3]). We write $\Delta_H\colon H \to H \otimes_A H$ and $\varepsilon_H\colon H \to A$ for the comultiplication and the counit. These give $\mathrm{Hom}_A(H, A')$ a structure of group with trivial element $H \xrightarrow{\varepsilon_H} A \to A'$, and (2.76.1) becomes a group isomorphism. An affine group scheme $\mathbf{G}$ is an *affine algebraic group* if A is a field and H is a finitely generated A-algebra.

Example 2.77. The most important example of affine group scheme is the general linear group. Let P be a finitely generated projective A-module. The *general linear group* of P is the group functor

$$\begin{array}{rl} \mathbf{GL}_{P/A}\colon \mathrm{Alg}_A \to \mathrm{Groups} & \\ A' \mapsto \mathrm{GL}_{A'}(P \otimes_A A')\,, & \end{array}$$

where $\mathrm{GL}_A(P \otimes_A A')$ denotes the group of A'-linear automorphisms of the A'-module $P \otimes_A A'$. It is an affine group scheme over A (see [18, Ch. II, §1, 2.4]). When P is a free A-module with a fixed basis $\{t_1, \ldots, t_n\}$, then one simply writes $\mathbf{GL}_{P/A} = \mathbf{GL}_n$. Note that, for any A-algebra A', $\mathbf{GL}_n(A')$ is the set of invertible $(m \times m)$-matrix with entries in A'. Conventionally, $\mathbf{GL}_0$ is the trivial A-scheme $\mathrm{Spec}(A)$. The Hopf algebra of $\mathbf{GL}_n$ can be naturally identified with

$$H := A[X_{i,j} : 1 \leq i, j \leq n]_{\det(X_{i,j})},$$

with the comultiplication and the counit given by

$$\Delta_H(X_{i,j}) = \sum_{k=1}^{n} X_{i,k} \otimes X_{k,j}, \quad \varepsilon_H(X_{i,j}) = \delta_{ij}.$$

Here the universal object $\sigma \in \mathbf{GL}_n(H)$ is given by the H-linear map $\sigma\colon P \otimes H \to P \otimes H$ such that

$$\sigma(t_j \otimes 1) = \sum_{i=1}^{n} t_i \otimes X_{i,j},$$

with associated matrix $(X_{i,j})$. The bijection $\mathrm{Hom}_A(H, A') \cong \mathbf{GL}_n(A')$ maps each homomorphism $\varphi \in \mathrm{Hom}_A(H, A')$ to the linear transformation $P \otimes_A A' \to P \otimes_A A'$ with associated matrix $(r_{i,j})$ at the given basis, where $r_{i,j} = \varphi(X_{i,j})$. Note also that, setting $A' = A$, the previous bijection $\mathrm{Hom}_A(H, A) \cong \mathbf{GL}_n(A)$ maps the counit ε_H to the identity.

2.78. *Closed subgroup schemes.* Let $\mathbf{G}$ be an affine group scheme over A with Hopf algebra H. We can view $\mathbf{G}$ as an affine scheme over A, namely $\mathrm{Spec}(H)$. In this regard, $\mathbf{G}$ becomes a group object in the category of schemes over A. We think of $\mathbf{G}$ interchangeably as a functor or as an affine scheme over A. A *closed subgroup* of $\mathbf{G}$ is an affine group scheme $\mathbf{G}'$ such that $\mathbf{G}'(A')$ is a subgroup of $\mathbf{G}(A')$ for every A-algebra A' and such that the inclusion $\mathbf{G}' \to \mathbf{G}$ is a closed immersion. The Hopf algebra H' of $\mathbf{G}'$ is therefore a quotient of H and the comultiplication, and the counit of H' are induced by the comultiplication and the counit of H.

2.79. *Quotient space of a group scheme over a field.* Let $\mathbf{G}$ be an affine algebraic group over a field K and let $\mathbf{H} \subset \mathbf{G}$ be a closed subgroup. A *quotient space* of $\mathbf{G}$ by $\mathbf{H}$ is an algebraic K-scheme $\mathcal{X}$ together with an action $\mathbf{G} \times \mathcal{X} \to \mathcal{X}$ and a rational point $o \in \mathcal{X}(K)$ such that for any K-algebra A':

(i) $\mathbf{H}(A') = \{g \in \mathbf{G}(A') : g \cdot o = o\}$, where o is viewed as element of $\mathcal{X}(A')$, and

(ii) for any $x \in \mathcal{X}(A')$ there is a faithfully flat A'-algebra A'' and $g' \in \mathbf{G}(A'')$ such that $x = g' \cdot o$, where both x and o are viewed as elements of $\mathcal{X}(A'')$.

A quotient space always exist for affine groups $\mathbf{H} \subset \mathbf{G}$ as above, and it is unique up to K-isomorphism (see [48, Appendix B]). The quotient space is denoted by $\mathbf{G}/\mathbf{H}$. Some interesting properties of $\mathbf{G}/\mathbf{H}$ are that it has dimension $\dim \mathbf{G} - \dim \mathbf{H}$ and that it is smooth over K if $\mathbf{G}$ is so (see [18, Ch. III, §3]).

2.80. *Automorphism group scheme and some subgroups.* Let A be a ring and C be a finitely generated projective A-module that has the structure of a (not necessarily commutative nor associative) A-algebra. In other words, C is a finitely generated projective A-module with an A-linear map $m_C\colon C \otimes_A C \to C$, $x \otimes y \mapsto xy$, called *multiplication*. Let $\mathcal{M}$ be a collection of A-submodules of C such that for each $M \in \mathcal{M}$ the quotient C/M is a projective A-module. In particular, each $M \otimes_A A'$ can be seen as an A'-submodule of $C \otimes_A A'$ for any $A' \in \mathrm{Alg}_A$. We define a group functor

$$\begin{aligned}\mathbf{Aut}_{C/A,\mathcal{M}}\colon \mathrm{Alg}_A &\to \mathrm{Groups}\\ A' &\to \mathrm{Aut}_{A',\mathcal{M}}(C \otimes_A A')\,,\end{aligned}$$

where $\mathrm{Aut}_{A',\mathcal{M}}(C \otimes_A A')$ is the group of A'-linear maps $\tau \in \mathbf{GL}_{C/A}(A') = \mathrm{GL}_{A'}(C \otimes_A A')$ satisfying the following two conditions:

(1) τ is respectful with the multiplication of $C \otimes_A A'$ as A'-algebra, that is, for any $x, y \in C$, we have $\tau(xy \otimes 1) = \tau(x \otimes 1)\tau(y \otimes 1)$.

(2) $\tau(M \otimes_A A') \subseteq M \otimes_A A'$, for any $M \in \mathcal{M}$. Since $C \otimes_A A'$ and $(C \otimes_A A')/(M \otimes_A A')$ are both finitely generated projective A'-modules, this is the same as requiring $\tau(M \otimes_A A') = M \otimes_A A'$.

Observe that if C has an identity 1, then any $\tau \in \mathbf{Aut}_{C/A,\mathcal{M}}(A') = \mathrm{Aut}_{A',\mathcal{M}}(C \otimes_A A')$ will automatically satisfy $\tau(1 \otimes 1) = 1 \otimes 1$.

We simply write $\mathbf{Aut}_{C/A}$ for $\mathbf{Aut}_{C/A,\emptyset} = \mathbf{Aut}_{C/A,\{C\}}$. This group-valued functor is in fact an affine group scheme of finite type over A (see [18, Ch. II, §1, 2.6]). In other words, the Hopf algebra of $\mathbf{Aut}_{C/A}$ is a finitely generated A-algebra.

We have seen in Example 2.77 that $\mathbf{GL}_{C/A}$ is an affine group scheme over A. By definition, we have an inclusion of group functors $\mathbf{Aut}_{C/A,\mathcal{M}} \subset \mathbf{GL}_{C/A}$ such that $\mathbf{Aut}_{C/A,\mathcal{M}}(A')$ is a subgroup of $\mathbf{GL}_{C/A}(A')$ for any A-algebra A'. We show that indeed the inclusion of functors induces an structure of closed subgroup scheme.

Proposition 2.81. *The group scheme* $\mathbf{Aut}_{C/A,\mathcal{M}}$ *is a closed subgroup of* $\mathbf{GL}_{C/A}$.

Proof. We have to show that $\mathbf{Aut}_{C/A,\mathcal{M}}$ is representable and that the inclusion $\mathbf{Aut}_{C/A,\mathcal{M}} \to \mathbf{GL}_{C/A}$ is a closed immersion. Note that $\mathbf{Aut}_{C/A,\mathcal{M}} = \cap_{M\in\mathcal{M}} \mathbf{Aut}_{C/A,\{M\}}$. Hence, we may assume that $\mathcal{M} = \{M\}$.

We begin by setting some notation. We denote by $m\colon C \otimes_k C \to C$ the multiplication of C, and for any $A' \in \mathrm{Alg}_A$ we denote by $m_{A'}\colon (C \otimes_A A') \otimes_{A'} (C \otimes_A A') \to C \otimes_A A'$ the A'-linear extension of m to a multiplication of $C \otimes_A A'$. Let $\iota\colon M \to C$ and $\pi\colon C \to C/M$ be respectively the inclusion and the quotient maps.

Let H be the Hopf algebra of $\mathbf{GL}_{C/A}$ and $\sigma \in \mathbf{GL}_{C/A}(H) = \mathrm{GL}_H(C \otimes_A H)$ be the universal H-linear automorphism. For any commutative A-algebra A', we have a natural bijection

$$\begin{aligned}\mathrm{Hom}_A(H, A') &\cong \mathbf{GL}_{C/A}(A')\\ \varphi &\mapsto \Big(C \otimes_A A' \xrightarrow{\sigma_\varphi} C \otimes_A A'\Big)\Big(\end{aligned} \tag{2.81.1}$$

where $\sigma_\varphi(c\otimes 1) = (\mathrm{id}_C\otimes\varphi)(\sigma(c\otimes 1))$ for any $c\in C$. In other words, σ_φ is the base change $\sigma\otimes_A A'_\varphi$ if we make use of the identification $C\otimes_A H\otimes_H A'_\varphi = C\otimes_A A'$. Note that

$$\sigma_\varphi \in \mathbf{Aut}_{C/A,\{M\}}(A') \quad\Leftrightarrow\quad \begin{aligned}&\sigma_\varphi\circ m_{A'} = m_{A'}\circ(\sigma_\varphi\otimes_{A'}\sigma_\varphi), \quad\text{and}\\ &(\pi\otimes_A A')\circ\sigma_\varphi\circ(\iota\otimes_A A') = 0.\end{aligned} \tag{2.81.2}$$

In fact $\sigma_\varphi\circ m_{A'} = m_{A'}\circ(\sigma_\varphi\otimes_{A'}\sigma_\varphi)$ says that σ_φ is compatible with the multiplication of the A'-algebra $C\otimes_A A'$, and $(\pi\otimes_A A')\circ\sigma_\varphi\circ(\iota\otimes_A A') = 0$ ensures that $\sigma_\varphi(M\otimes_A A')\subset M\otimes_A A'$.

We now consider the maps of H-modules

$$\begin{aligned}&\Phi\colon (C\otimes_A H)\otimes_H(C\otimes_A H)\xrightarrow{\sigma\circ m_H - m_H\circ(\sigma\otimes_H\sigma)} C\otimes_A H,\\ &\Psi\colon M\otimes_A H\xrightarrow{(\pi\otimes_A\mathrm{id}_H)\circ\sigma\circ(\iota\otimes_A\mathrm{id}_H)}(C/M)\otimes_A H.\end{aligned}$$

Observe that given $A'\in\mathrm{Alg}_A$ and $\varphi\in\mathrm{Hom}_A(H,A')$, the base changes $\Phi\otimes_H A'_\varphi$ and $\Psi\otimes_H A'_\varphi$ are respectively

$$\sigma_\varphi\circ m_{A'} - m_{A'}\circ(\sigma_\varphi\otimes_{A'}\sigma_\varphi) \quad\text{and}\quad (\pi\otimes_A A')\circ\sigma_\varphi\circ(\iota\otimes_A A').$$

It follows from (2.81.2) that, under the identification (2.81.1),

$$\mathbf{Aut}_{C/A,\{M\}}(A')\cong\{\varphi\in\mathrm{Hom}_A(H,A') : \Phi\otimes_H A'_\varphi = 0 \quad\text{and}\quad \Psi\otimes_H A'_\varphi = 0\}.$$

Since $C\otimes_A H$ and $(C/M)\otimes_A H$ are finitely generated projective H-modules, we can apply [24, Proposition 8.4] to conclude that $\mathbf{Aut}_{C/A,\{M\}}$ is a closed subgroup of $\mathbf{GL}_{C/A}$. This completes the proof. □

Remark 2.82. The automorphism group schemes $\mathbf{Aut}_{C/A,\mathcal{M}}$ behave well under base change. In other words, for any A-algebra A', we have

$$\mathbf{Aut}_{C'/A',\mathcal{M}'} = \mathbf{Aut}_{C/A,\mathcal{M}}\times_A\mathrm{Spec}(A')$$

where $C' := C\otimes_A A'$ and $\mathcal{M}' := \{M\otimes_A A' : M\in\mathcal{M}\}$.

The automorphism group schemes of finite dimension algebras over a perfect field is widely studied in [19]. In particular, they introduce conditions on C that ensure that $\mathbf{Aut}_{C/k}$ is reduced and hence smooth.

2.3.3. Automorphism group scheme of an extension with splitting p-basis

We assume all the rings to be of characteristic p in this subsection. We study the automorphism group scheme of an extension with splitting p-basis. That is, we analyse $\mathbf{Aut}_{C/A}$ where $C = A[X_1,\dots,X_n]/\langle X_1^p,\dots,X_n^p\rangle$ for some ring A. We will consider some specific subgroups $\mathbf{Aut}_{C/A,\mathcal{M}}$ of $\mathbf{Aut}_{C/A}$ that will be used later in the construction of the Yuan scheme.

The extensions with splitting p-basis belong to the class of purely inseparable extensions of rings. The automorphism group schemes of this class of extensions have been considered in the literature with different perspectives. The case of finite purely inseparable field extensions was discussed by L. Bégueri ([5]), S. Shatz ([60]) and S. U. Chase ([16]) in connection with Galois theory. More recently, the general case of finite purely inseparable ring extensions was considered by F. Sancho de Salas and P. Sancho de Salas in [55], where they gave a criterion for the automorphism group to be integral.

In what follows, let $A \subseteq C$ be a finite extension with splitting p-basis, that is, with C of the form

$$C = A[X_1, \dots, X_n]/\langle X_1^p, \dots, X_n^p \rangle.$$

Denote by x_i the class of X_i in C, so $\{x_1, \dots, x_n\}$ is a splitting p-basis for C over A. Let $\mathfrak{m} = \langle x_1, \dots, x_n \rangle \subset C$ be the maximal ideal, and, for a fixed $0 \leq r < n$, let

$$B = A[x_{r+1}, \dots, x_n] \subset C.$$

We consider the group-valued subfunctors $\mathbf{Aut}_{C/A,\{B,\mathfrak{m}\}} \subset \mathbf{Aut}_{C/A,\{B\}} \subset \mathbf{Aut}_{C/A}$, that attach to each A-algebra A' the sets

$$\mathbf{Aut}_{C/A,\{B\}}(A') := \{\sigma \in \mathrm{Aut}_{A'}(C \otimes_A A') \colon \sigma(B \otimes_A A') = B \otimes_A A'\},$$
$$\mathbf{Aut}_{C/A,\{B,\mathfrak{m}\}}(A') := \left\{\sigma \in \mathrm{Aut}_{A'}(C \otimes_A A') \colon \begin{array}{l} \sigma(B \otimes_A A') = B \otimes_A A', \\ \sigma(\mathfrak{m} \otimes_A A') = \mathfrak{m} \otimes_A A' \end{array}\right\}\Bigg($$

We already know by Proposition 2.81, that they are closed subgroups of $\mathbf{GL}_{C/A}$. We can elaborate further and show that these subfunctors are indeed closed subgroups of $\mathbf{Aut}_{C/A}$. Indeed, we identify the group schemes that represent them.

Proposition 2.83. *The group schemes $\mathbf{Aut}_{C/A,\{B\}}$ and $\mathbf{Aut}_{C/A,\{B,\mathfrak{m}\}}$ are representable by closed subgroups of $\mathbf{Aut}_{C/A}$. Moreover,*

(1) $\mathbf{Aut}_{C/A,\{B,\mathfrak{m}\}}$ is isomorphic to $\mathbf{GL}_r \times \mathbf{GL}_{n-r} \times \mathbb{A}_A^t$ as scheme over A, where

$$t + r^2 + (n-r)^2 = (p^n - 1)r + (p^{n-r} - 1)(n-r).$$

(2) $\mathbf{Aut}_{C/A,\{B\}} \simeq \mathbf{Aut}_{C/A,\{B,\mathfrak{m}\}} \times \mathrm{Spec}(C)$ as schemes over A.

Proof. Let $\mathbf{e}_1, \dots, \mathbf{e}_n$ be the canonical vectors of $\mathbb{N}_0^n$ and write $\mathbf{0} := (0, \dots, 0)$. We set

$$\mathcal{A} := \{\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n : 0 \leq \alpha_i < p\}, \quad \mathcal{A}_+ := \mathcal{A} \backslash \{\mathbf{0}\},$$

$$\mathcal{B} := \{\beta \in \mathcal{A} : \beta_i = 0 \quad \text{for } i \leq r\}, \quad \mathcal{B}_+ := \mathcal{B} \cap \mathcal{A}_+.$$

Let A' be a fixed A-algebra and set $y_i := x_i \otimes 1$ for $i = 1, \dots, n$. Then $\{y_1, \dots, y_n\}$ is a splitting p-basis for $C \otimes_A A'$ over A' and the elements $y_{r+1}, \dots, y_n$ generate $B \otimes_A A'$ as A'-algebra (Lemma 2.25.(2)). Note that any endomorphism of A'-algebras $\tau \colon C \otimes_A A' \to C \otimes_A A'$ satisfying $\tau(B \otimes_A A') \subseteq B \otimes_A A'$ is completely determined by its values $\tau(y_1), \dots, \tau(y_n)$. The possible values for these images are any elements

$f_1, \dots, f_n \in C \otimes_A A'$ such that $f_i^p = 0$, for $i = 1, \dots, n$, and $f_{r+1}, \dots, f_n \in B \otimes_A A'$. Thus, $f_1, \dots, f_n$ can be any elements of the form

$$f_i := a_{i,\mathbf{0}} + \sum_{\alpha \in \mathcal{A}_+} a_{i,\alpha} \mathbf{y}^\alpha, \quad \text{for } i = 1, \dots, r,$$

$$f_i := a_{i,\mathbf{0}} + \sum_{\beta \in \mathcal{B}_+} a_{i,\beta} \mathbf{y}^\beta, \quad \text{for } i = r+1, \dots, n,$$

with $a_{i,\alpha}, a_{i,\beta} \in A'$ and $a_{i,\mathbf{0}}^p = 0$ for $i = 1, \dots, n$ and $\alpha \in \mathcal{A}_+$ and $\beta \in \mathcal{B}_+$.

As we want τ to be an automorphism, we have to determine when is bijective. Since $C \otimes_A A'$ is a finitely generated A'-module, this is the same as requiring that τ is surjective. Then we have to show when $f_1, \dots, f_n$ generate $C \otimes_A A'$ as an A'-algebra, equivalently, when $f_i^+ := f_i - a_{i,\mathbf{0}}$, $i = 1, \dots, n$, generate $C \otimes_A A'$ as A'-algebra. Since $\mathfrak{m} \otimes_A A'$ is nilpotent, by Proposition A.36 this is the same as requiring that the classes of $f_1^+, \dots, f_n^+ \in \mathfrak{m} \otimes_A A'$ modulo $\mathfrak{m}^2 \otimes_A A'$ generate the A'-module $(\mathfrak{m}/\mathfrak{m}^2) \otimes_A A'$, which is a free A'-module of rank n. Thus, it follows that τ is bijective if and only if $(a_{i,\mathbf{e}_j})_{1 \le i,j \le n} \in \mathbf{GL}_n(A')$. Recall that $a_{i,\mathbf{e}_j} = 0$ if $j \le r$ and $i > r$, so we have $(a_{i,\mathbf{e}_j})_{1 \le i,j \le n} \in \mathbf{GL}_n(A')$ if and only if $(a_{i,\mathbf{e}_j})_{1 \le i,j \le r} \in \mathbf{GL}_r(A')$ and $(a_{i,\mathbf{e}_j})_{r+1 \le i,j \le n} \in \mathbf{GL}_{n-r}(A')$.

Finally, observe that $(a_{1,\mathbf{0}}, \dots, a_{n,\mathbf{0}})$ can be identified with the point of $\mathrm{Hom}_A(C, A')$ corresponding to the A-algebra homomorphism which maps x_i to $a_{i,\mathbf{0}}$. In addition, we have $\tau(\mathfrak{m} \otimes_A A') = \mathfrak{m} \otimes_A A'$ precisely when $a_{1,\mathbf{0}} = \cdots = a_{n,\mathbf{0}} = 0$. Then, there are natural bijections

$$\mathbf{Aut}_{C/A,\{B\}}(A') \cong \mathrm{Hom}_A(C, A') \times \mathbf{GL}_r(A') \times \mathbf{GL}_{n-r}(A') \times \prod_{i=1}^{r} (A')^{\mathcal{A}'} \times \prod_{i=r+1}^{n} (A')^{\mathcal{B}'},$$

$$\mathbf{Aut}_{C/A,\{B,\mathfrak{m}\}}(A') \cong \mathrm{Hom}_A(C/\mathfrak{m}, A') \times \mathbf{GL}_r(A') \times \mathbf{GL}_{n-r}(A') \times \prod_{i=1}^{r} (A')^{\mathcal{A}'} \times \prod_{i=r+1}^{n} (A')^{\mathcal{B}'},$$

where $\mathcal{A}' := \mathcal{A}_+ \backslash \{\mathbf{e}_1, \dots, \mathbf{e}_r\}$ and $\mathcal{B}' := \mathcal{B}_+ \backslash \{\mathbf{e}_{r+1}, \dots, \mathbf{e}_n\}$. The bijections above show that $\mathbf{Aut}_{C/A,\{B\}}$ is representable by the affine A-scheme

$$\mathrm{Spec}(C) \times \mathbf{GL}_r \times \mathbf{GL}_{n-r} \times \mathbb{A}_A^t,$$

where $t = r|\mathcal{A}'| + (n-r)|\mathcal{B}'|$, and $\mathbf{Aut}_{C/A,\{B,\mathfrak{m}\}}$ is represented by the closed subscheme $\mathbf{GL}_r \times \mathbf{GL}_{n-r} \times \mathbb{A}_A^t$. Since $|\mathcal{A}'| = p^n - r - 1$ and $|\mathcal{B}'| = p^{n-r} - 1 - (n-r)$, we conclude that

$$\begin{aligned} r^2 + (n-r)^2 + t &= r^2 + (n-r)^2 + r(p^n - r - 1) + (n-r)(p^{n-r} - 1 - (n-r)) \\ &= (p^n - 1)r + (p^{n-r} - 1)(n-r)\,, \end{aligned}$$

and the proof is complete. □

Remark 2.84. Since $\mathrm{Hom}_A(C, A') = \{(a_1, \dots, a_n) \in (A')^n \colon a_i^p = 0\}$ is an additive subgroup of $(A')^n$, the scheme $\mathrm{Spec}(C)$ is actually an affine group scheme. Moreover, $\mathrm{Spec}(C)$ can be identified with a subgroup of $\mathbf{Aut}_{C/A,\{B\}}$ as follows: each A'-point $(a_1, \dots, a_n) \in \mathrm{Spec}(C)(A') = \mathrm{Hom}_A(C, A')$ can be identified with the A'-automorphism $\tau \in \mathbf{Aut}_{C/A,\{B\}}(A')$ such that $\tau(x_i \otimes 1) = a_i + x_i \otimes 1$.

Using the isomorphisms given in Proposition 2.83 we can deduce some geometric properties of the automorphisms group schemes.

Corollary 2.85. *If K is a field, then $\mathbf{Aut}_{C/K,\{B,\mathfrak{m}\}}$ is smooth and geometrically irreducible of dimension $(p^n-1)r+(p^{n-r}-1)(n-r)$. In addition, it is the reduced scheme of $\mathbf{Aut}_{C,\{B\}}$.*

Proof. The first part of the corollary is a direct consequence of the isomorphism of K-schemes $\mathbf{Aut}_{C/K,\{B,\mathfrak{m}\}} \simeq \mathbf{GL}_r \times \mathbf{GL}_{n-r} \times \mathbb{A}^t_K$ from Proposition 2.83. It is clear also that $\mathbf{Aut}_{C/K,\{B,\mathfrak{m}\}}$ is a reduced subscheme of $\mathbf{Aut}_{C/k,\{B\}}$, since all the factors in the isomorphism are reduced. So, it only lefts to show that the map $\mathbf{Aut}_{C/K,\{B,\mathfrak{m}\}} \to \mathbf{Aut}_{C/K,\{B\}}$ is surjective on points. To prove this it is enough to show that $\mathbf{Aut}_{C/K,\{B,\mathfrak{m}\}}(\bar{K}) = \mathbf{Aut}_{C/K,\{B\}}(\bar{K})$, where $\bar{K}$ denotes an algebraic closure of K. This equality is clear, since the maximal ideal of the local ring $C \otimes_K \bar{K} = \bar{K}[X_1,\dots,X_n]/\langle X_1^p,\dots,X_n^p\rangle$ is $\mathfrak{m} \otimes_K \bar{K}$ and every automorphism of a local ring fixes the maximal ideal. □

Corollary 2.86. *If K is a field, then $\mathbf{Aut}_{C/K,\{B\}}$ is geometrically irreducible and has dimension $(p^n-1)r+(p^{n-r}-1)(n-r)$. It is not a reduced scheme except for the trivial case $n=0$.*

Proof. The first part of the corollary is just a consequence of Remark 2.82 and Corollary 2.85. We now prove the last part. By Proposition 2.81, we have an isomorphism $\mathbf{Aut}_{C/K,\{B\}} \simeq \mathbf{GL}_r \times \mathbf{GL}_{n-r} \times \mathbb{A}^t_K \times \mathrm{Spec}(C)$. Since K is a reduced ring, then all factors are reduced except for the last one that corresponds with the ring C. Note that C is non-reduced if $n>0$, since it has non-zero nilpotent elements. Thus, $\mathbf{Aut}_{C/K,\{B\}}$ is reduced only if $n=0$. □

2.3.4. Yuan scheme

In this subsection, we remain in the context of prime characteristic rings. We define a functor in order to parametrize the Galois towers of rings whose intermediate Galois subextensions have fixed rank. Following the results from [12, §4], we show that this functor is representable by an scheme and we study its geometric properties.

We begin by introducing the notion of differential rank of a Galois extension of exponent one.

Definition 2.87. A Galois extension of exponent one $A \subseteq C$ has *differential rank n* if the projective C-module $\Omega_{C/A}$ has constant rank n. Equivalently, if, for any prime ideal $\mathfrak{p} \subset A$, the length of any p-basis for $C_\mathfrak{p}$ over $A_\mathfrak{p}$ is n (Proposition 2.53).

Note that any trivial extension has differential rank zero. As direct consequence of Lemma 2.25 and Proposition 2.73, we obtain the following properties of the differential rank of Galois extensions.

Lemma 2.88. *Let $A \subseteq C$ be a Galois extension of exponent one and differential rank n.*

(1) *Let A' be an A-algebra. Then $A' \subseteq C \otimes_A A'$ is a Galois extension of differential rank n.*

(2) *Let B be an intermediate subring, i.e., $A \subseteq B \subseteq C$. If $B \subseteq C$ is a Galois extension of differential rank r, then $A \subseteq B$ is a Galois extension of differential rank $n - r$.*

We are interested also in the behaviour of splitting p-basis and Galois towers with fixed differential rank.

Proposition 2.89. *Let $A \subseteq C$ be a Galois extension of differential rank n. Let B be an intermediate subring, $A \subseteq B \subseteq C$, such that $B \subseteq C$ is a Galois extension of differential rank r. Then there exists a finitely presented and faithfully flat A-algebra A' such that $A' \subseteq C \otimes_A A'$ has a splitting p-basis $z_1, \ldots, z_n$ such that $B \otimes_A A' = A'[z_{r+1}, \ldots, z_n]$.*

Proof. We have that $A \subseteq B$ is a Galois extension of differential rank $n-r$ by Lemma 2.88.(2). In particular, $A \subseteq B \subseteq C$ is a Galois tower and the induced morphisms $\mathrm{Spec}(C) \to \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ are homeomorphisms (see Remark 2.2). Then applying Proposition 2.55 to both extensions $A \subseteq B$ and $B \subseteq C$, we deduce that there are $f_1, \ldots, f_s \in A$ generating the unit ideal such that B_{f_i} has a p-basis $\{x_{r+1}^{(i)}, \ldots, x_n^{(i)}\}$ over A_{f_i} and C_{f_i} has a p-basis $\{x_1^{(i)}, \ldots, x_r^{(i)}\}$ over B_{f_i}, for each $i = 1, \ldots, s$. Hence, $\{x_1^{(i)}, \ldots, x_n^{(i)}\}$ is a p-basis of C_{f_i} over A_{f_i} by Lemma 2.25.(3).

We can apply Proposition 2.27 to the extension $A_{f_i} \subseteq C_{f_i}$, the p-basis $\{x_1^{(i)}, \ldots, x_n^{(i)}\}$ and $A' = C_{f_i}$, so the set $\{z_1^{(i)}, \ldots, z_n^{(i)}\}$, where

$$z_j^{(i)} := x_j^{(i)} \otimes 1 - 1 \otimes x_j^{(i)} \in C_{f_i} \otimes_{A_{f_i}} C_{f_i} = C \otimes_A C_{f_i},$$

is a splitting p-basis of $C \otimes_A C_{f_i}$ over C_{f_i}. It is clear that $B \otimes_A C_{f_i} = C_{f_i}[z_{r+1}^{(i)}, \ldots, z_n^{(i)}]$.

We set $A' := C_{f_1} \times \cdots \times C_{f_s}$ and define $z_j := (z_j^{(1)}, \ldots, z_j^{(s)}) \in C \otimes_A A'$ for $j = 1, \ldots, n$. Observe that $\{z_1, \ldots, z_n\}$ is a splitting p-basis for $C \otimes_A A'$ over A' and that $B \otimes_A A' = A'[z_{r+1}, \ldots, z_n]$. Thus, it only lefts to show that $A \to A'$ is finitely presented and faithfully flat. Note that the localization $A \to A_{f_i}$ is flat of finite presentation. The same happens for the extension $A_{f_i} \subset C_{f_i}$ since C_{f_i} is a finite projective A_{f_i}-module (see Proposition 1.7). Hence, the composition $A \to C_{f_i}$ is also finitely presented and flat (see Proposition A.28 and Proposition A.17). It follows that the induced homomorphism $A \to A'$ is flat of finite presentation since $A' = C_{f_1} \times \cdots \times C_{f_s}$. Finally, note that the induced morphism $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$ is surjective, thus A' is a faithfully flat A-algebra by Proposition A.19, as we wanted. □

Now, we define the functor whose points are the Galois towers of rings whose intermediate Galois subextensions have fixed differential rank.

Definition 2.90. Let $A \subseteq C$ be a Galois extension of differential rank n. Fix an integer $0 \leq r \leq n$. The *Yuan functor* associated to $A \subseteq C$ and r is the covariant

functor from the category of A-algebras to the category of sets given by

$$\mathcal{Y}^r_{C/A}\colon \mathrm{Alg}_A \to \mathrm{Sets}$$
$$A' \mapsto \left\{ B' : \begin{array}{l} A' \subseteq B' \subseteq C \otimes_A A', \\ B' \subseteq C \otimes_A A' \text{ is Galois of differential rank } r \end{array} \right\}.$$

Note that for any $B' \in \mathcal{Y}^r_{C/A}(A')$, the extension $A' \subseteq B'$ is Galois of differential rank $n - r$ (Lemma 2.88).

Remark 2.91. By definition, the Yuan functor behaves well under base change. That is, if A' is an A-algebra and $C' := C \otimes_A A'$, then $\mathcal{Y}^r_{C'/A'} = \mathcal{Y}^r_{C/A} \times_A \mathrm{Spec}(A')$.

We show that $\mathcal{Y}^r_{C/A}$ is representable by a quasi-projective A-scheme. This fact is a consequence of Theorem 1.36 on the representability of the Grassmannian functor of subalgebras, since any Galois tower of fixed differential rank is in particular a finite projective tower of rings of fixed constant rank.

Theorem 2.92. *Let $A \subseteq C$ be a Galois extension of differential rank n. Fix a non-negative integer $r \leq n$. Then the Yuan functor $\mathcal{Y}^r_{C/A}$ is representable by a quasi-projective A-scheme.*

Proof. By the definition of p-basis, it is clear that any Galois extension $A' \subseteq C'$ has differential rank m if and only if C' has rank p^m as A'-module. In particular, C has rank p^n as A-module. From this observation and Proposition 2.73, we deduce that $\mathcal{Y}^r_{C/A} = \mathcal{G}^q_{C/A}$ with $q = p^r$. Therefore, the representability of $\mathcal{Y}^r_{C/A}$ by a quasi-projective A-scheme follows from Theorem 1.36. □

Since $\mathcal{Y}^r_{C/A}$ is representable, we abuse of notation and call it also the *Yuan scheme*. We show in the following example that the Yuan scheme $\mathcal{Y}^r_{C/A}$ might not be projective over A.

Example 2.93. Let $K = \overline{\mathbb{F}_2}$ and $C = K[X,Y]/\langle X^2, Y^2\rangle$. Then $C = K \oplus Kx \oplus Ky \oplus Kxy$, where x and y denote the class of X and Y, respectively. An element of $B \in \mathcal{Y}^1_{C/K}(K)$ is an intermediate subring $K \subset B \subset C$ such that $B \subset C$ is Galois of differential rank 1. In particular, C is flat over B (Proposition 1.7). Recall that C is differentiably simple by Example 2.32. Then B is also differentiably simple by Proposition 2.37. Moreover, B has the form $K \oplus K(ax+by+cxy)$ for some $a, b, c \in K$ with $a \neq 0$ or $b \neq 0$ by Corollary 2.40. Therefore, $\mathcal{Y}^1_{C/K}(k)$ is isomorphic as a variety to $\{[a:b:c] \in \mathbb{P}^2(K) : a \neq 0 \text{ or } b \neq 0\} \subset \mathbb{P}^2(K)$, which is clearly not projective.

Finally, we study some relevant geometric properties of the Yuan scheme $\mathcal{Y}^r_{C/A}$. We begin by analysing the fibers of the structural morphism $\mathcal{Y}^r_{C/A} \to \mathrm{Spec}(A)$. As we noted in Remark 2.91, the Yuan scheme behaves well under base change. Thus, we can analyse instead the Yuan scheme $\mathcal{Y}^r_{C/A}$ when $A = K$ is a field.

We begin with the particular case in which C is a differentiably simple ring of the form

$$C = K[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p\rangle =: k[x_1, \ldots, x_n],$$

for a field K. Let $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$ be the maximal ideal of C and $B = k[x_{r+1}, \ldots, x_n]$ for some fixed $0 \leq r < n$. In particular, $B \in \mathcal{Y}^r_{C/K}(K)$. We will show that $\mathcal{Y}^r_{C/k}$ is a quotient space of $\mathbf{Aut}_{C/k}$. With this aim, we consider the natural action of the algebraic group $\mathbf{Aut}_{C/K}$ on the Yuan scheme $\mathcal{Y}^r_{C/K}$ given for any K-algebra A' by

$$\begin{aligned} \mathbf{Aut}_{C/K}(A') \times \mathcal{Y}^r_{C/K}(A') &\to \mathcal{Y}^r_{C/K}(A') \\ (\tau, B') &\mapsto \tau(B')\,. \end{aligned}$$

Proposition 2.94. *In the setting described above, the natural action of the subgroup $\mathbf{Aut}_{C/K,\{\mathfrak{m}\}} \subset \mathbf{Aut}_{C/K}$ on $\mathcal{Y}^r_{C/K}$ induces a K-isomorphism of schemes*

$$\mathbf{Aut}_{C/K,\{\mathfrak{m}\}}/\mathbf{Aut}_{C/K,\{B,\mathfrak{m}\}} \cong \mathcal{Y}^r_{C/K}.$$

Therefore, $\mathcal{Y}^r_{C/K}$ is smooth over K and irreducible of dimension $(p^n - p^{n-r})(n-r)$.

Proof. Since the quotient space is unique up to K-isomorphism (see discussion 2.79), the proposition follows if we prove that $\mathcal{Y}^r_{C/K}$ with the rational point $B \in \mathcal{Y}^r_{C/K}(K)$ verify the conditions on the definition of the quotient space $\mathbf{Aut}_{C/k,\{\mathfrak{m}\}}/\mathbf{Aut}_{C/k,\{B,\mathfrak{m}\}}$. In other words, we have to show that for any K-algebra A' the next conditions hold:

(i) $\mathbf{Aut}_{C/K,\{B,\mathfrak{m}\}}(A') = \{\tau \in \mathbf{Aut}_{C/K,\{\mathfrak{m}\}}(A') : \tau(B \otimes_K A') = B \otimes_K A'\}$, and

(ii) for any $B' \in \mathcal{Y}^r_{C/K}(A')$ there is a faithfully flat A'-algebra A'' and a map $\tau \in \mathbf{Aut}_{C/K,\{\mathfrak{m}\}}(A'')$ such that $B' = \tau(B)$, where both B' and B are viewed as elements of $\mathcal{Y}^r_{C/K}(A'')$.

The first condition is clear by the definition of $\mathbf{Aut}_{C/K,\{B,\mathfrak{m}\}}(A')$. So we only have to verify (ii). Let $B' \in \mathcal{Y}^r_{C/K}(A')$. Then $A' \subseteq B'$ and $B' \subseteq C \otimes_K A'$ are Galois extensions of differential ranks $n-r$ and r respectively (see Lemma 2.88). An application of Proposition 2.89 to these extensions ensures that there exists a finitely presented and faithfully flat A'-algebra A'' and a splitting p-basis $\{z_1, \ldots, z_n\}$ for $C \otimes_K A' \otimes_{A'} A'' = C \otimes_K A''$ over A'' such that $B' \otimes_K A'' = A''[z_{r+1}, \ldots, z_n]$. We can use the decomposition $C \otimes_K A'' = A'' \oplus (\mathfrak{m} \otimes_K A'')$ to assume that $z_1, \ldots, z_n \in \mathfrak{m} \otimes_K A''$, so that $\langle z_1, \ldots, z_n \rangle = \mathfrak{m} \otimes_K A''$. Finally, denote by y_i the image of $x_i \in C$ in $C \otimes_K A''$, then the assignation $y_i \mapsto z_i$ for each $i = 1, \ldots, n$, induces an A''-automorphism of $C \otimes_K A''$ sending $\mathfrak{m} \otimes_K A''$ onto itself and $B \otimes_K A''$ onto $B \otimes_K A''$. Thus condition (ii) is satisfied and the isomorphism between $\mathcal{Y}^r_{C/k}$ and the quotient space is proved.

Finally, we prove that $\mathcal{Y}^r_{C/K}$ satisfies the geometric properties from the statement. We know that $\mathbf{Aut}_{C/K,\{\mathfrak{m}\}}$ is smooth over k and irreducible (by Corollary 2.85 with $r = 0$). Thus, as we noted in discussion 2.79, the same holds for $\mathcal{Y}^r_{C/K}$. In addition, using the dimensions computed in 2.85, we conclude that $\dim \mathcal{Y}^r_{C/K} = \dim \mathbf{Aut}_{C/K,\{\mathfrak{m}\}} - \dim \mathbf{Aut}_{C/K,\{\mathfrak{m},B\}} = (p^n - p^{n-r})(n-r)$. □

Finally, we return to the general situation where $A \subseteq C$ is a Galois extension of fixed differential rank. Using the above proposition, we deduce the geometric properties for the Yuan scheme in general.

Theorem 2.95. *Let $A \subseteq C$ be a Galois extension of exponent one and differential rank n. Fix a positive integer $r < n$. Then the Yuan scheme $\mathcal{Y}^r_{C/A}$ is smooth over* $\mathrm{Spec}(A)$ *and has smooth irreducible fibers of dimension $(p^n - p^{n-r})(n-r)$. In addition, if* $\mathrm{Spec}(A)$ *is irreducible (i.e., has a unique generic point), so is $\mathcal{Y}^r_{C/A}$.*

Proof. By Proposition 2.89, there exists a finitely presented faithfully flat A-algebra A' such that $C' := C \otimes_A A' \cong A'[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$ for some $n \geq 0$. Since $\mathcal{Y}^r_{C'/A'} \cong \mathcal{Y}^r_{C/A} \times_A \mathrm{Spec}(A')$ as we noted in Remark 2.91, in order to show that $\mathcal{Y}^r_{C/A}$ is smooth over A it is enough to show that $\mathcal{Y}^r_{C'/A'}$ is smooth over A'. Observe that $A' \subseteq C'$ is a base change of the extension $\mathbb{F}_p \subseteq \mathbb{F}_p[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p \rangle$. Since the Yuan scheme attached to this extension is smooth by 2.94, we conclude that $\mathcal{Y}_{C'/A'}$ is also smooth over $\mathrm{Spec}(A')$. The smoothness of the fibers and the formula for the dimension follow also from Proposition 2.94.

Finally, we assume that $\mathrm{Spec}(A)$ is irreducible. Since $\mathcal{Y}^r_{C/A} \to \mathrm{Spec}(A)$ is smooth, it is in particular open, then the fiber over the generic point of $\mathrm{Spec}(A)$ is irreducible by Proposition 2.94. We conclude that $\mathcal{Y}^r_{C/A}$ is irreducible by [24, Proposition 3.24]. □

CHAPTER 3

Purely inseparable extensions of higher exponent

We have already studied purely inseparable ring extensions of exponent at most one, or Galois extensions, in Chapter 2. Now we dedicate this chapter to the study of *purely inseparable extensions* of arbitrary finite exponent, that is, commutative ring extensions with unity $A \subseteq C$ of prime characteristic p such that

(i) $C^{p^e} \subseteq A$ for some $e \geq 0$;

(ii) C is a finitely generated and projective A-module; and

(iii) for each prime ideal $\mathfrak{p} \subset A$, there is a faithfully flat ring extension $A_{\mathfrak{p}} \to A'$ such that $C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A'$ is isomorphic to an A'-algebra $A'[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$ for some $n \geq 0$ and $e_i > 0$.

This notion extends the notion of purely inseparable field extension to the setting of rings. Purely inseparable extensions of fields have been widely studied by many authors as S. Shatz ([60]), S. U. Chase ([16]) and G. Pickert ([51], [52]). The particular case of purely inseparable ring extensions $A \subseteq C$ in which A is a field was treated by R. Rasala in [54]. Then F. Pauer ([49]) introduced the general case of purely inseparable ring extensions under the name of *special algebras*. His original definition contemplated a series of equivalent conditions ([49, Satz 2.2.5]) that can be seen as an extension to the higher exponent case of some of the equivalences from Theorem 2.71 for purely inseparable extensions of exponent one. On the one hand, he gave a condition for higher exponent extensions that might be seen as a generalization of the exponent-one extension's property of having a p-basis locally, at any prime ideal. Namely, he proved that condition (iii) in the above definition can be replaced by the next property:

(iv) for each prime ideal $\mathfrak{p} \subset A$, there is a presentation $C_{\mathfrak{p}} = A_{\mathfrak{p}}[x_1, \ldots, x_n]$ as $A_{\mathfrak{p}}$-algebra, whose defining relations are $x_i^{p^{e_i}} = P_i(x_1^{p^{e_i}}, \ldots, x_{i-1}^{p^{e_i}})$ for some positive integers $e_1 \geq \cdots \geq e_n$ and polynomials $P_i \in A[X_1, \ldots, X_{i-1}]$.

On the other hand, he studied the connection between purely inseparable extensions and the modules of differentials. More precisely, he proved that purely inseparable

extensions are finite ring extensions of finite exponent such that the module of differentials $\Omega_{A[C^{p^e}]/A}$ is a projective $A[C^{p^e}]$-module for all $e \geq 0$. Later on, P. Sancho de Salas recovered in [56] the relation between the modules of differentials and the modules of principal parts. He proved that purely inseparable extensions are finite ring extensions of finite exponent such that the C-module of principal parts $\mathrm{P}^k_{C/A}$ is projective for all $k \geq 0$.

Our first interest is to extend the characterizations of Galois extensions of exponent one from Theorem 2.71 to purely inseparable extensions of higher exponent. First, we review the mentioned characterizations from F. Pauer that already extend the equivalences (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (4) from Theorem 2.71. Then we study the connection between differential operators and purely inseparable extensions that expands the connection between derivations and Galois extensions previously treated in Subsection 2.2.3 from the second chapter. We prove a result on extensions of differential operators, which is the key to give a new characterization of purely inseparable extensions in terms of some modules of differential operators, that extends the equivalence (1) $\Leftrightarrow$ (6) from Theorem 2.71. Specifically, we show that a finite ring extension of finite exponent is purely inseparable if and only if C is a projective $A[C^{p^e}]$-module for all $0 \leq e < \exp(C/A)$, and the module of differential operators $\mathrm{Diff}^k_A(C)$ is a C-module direct summand of $\mathrm{End}_A(C)$ for all $k \geq 0$. Moreover, using these techniques on differential operators, we re-obtain from a different perspective the characterization in terms of the modules of principal parts. In particular, we show that a finite ring extension of finite exponent is purely inseparable if and only if the C-module of principal parts $\mathrm{P}^{p^e}_{C/A}$ is projective for all $0 \leq e < \exp(C/A)$.

Our second interest is to study *purely inseparable towers of rings*, that is, towers of rings $A \subseteq B \subseteq C$ such that $A \subseteq B$, $B \subseteq C$ and $A \subseteq C$ are purely inseparable extensions. In Section 2.3 from the second chapter, we have discussed the exponent one case.

On the one hand, given $A \subseteq C$ a Galois extension of rings and B an intermediate subring, we have shown that $A \subseteq B \subseteq C$ is a Galois tower if and only if C is projective as a B-module. The situation is more complicated for purely inseparable extensions of higher exponent. Namely, if $A \subseteq C$ is a purely inseparable ring extension of exponent greater than one and B is an intermediate subring such that C is projective as B-module, then it is not necessarily true that $A \subseteq B$ and $B \subseteq C$ are also purely inseparable. Thus, given a purely inseparable ring extension $A \subseteq C$ and a intermediate subring B, we look for conditions that ensure that both subextension $A \subseteq B$ and $B \subseteq C$ are purely inseparable, equivalently, that $A \subseteq B \subseteq C$ is a purely inseparable tower.

On the other hand, given two Galois extensions of rings $A \subseteq B$ and $B \subseteq C$, we know that $A \subseteq C$ is also Galois if it has exponent at most one. However, it is not that simple for purely inseparable extensions of higher exponent. Therefore, given two purely inseparable extensions $A \subseteq B$ and $B \subseteq C$, we try to answer the question of whether the extension $A \subseteq C$ is also purely inseparable, and so $A \subseteq B \subseteq C$ is a purely inseparable tower.

Organization. This chapter is divided into three sections. The first one studies purely inseparable extensions of rings from the original perspective of F. Pauer ([49]). The purpose of the second section is to approach purely inseparable ring extensions from the perspective of differential operators and modules of principal parts. The third section addresses towers of purely inseparable extensions. The content of these two last sections corresponds to the results presented in [11], which are joint work of the author of this thesis and D. Sulca.

Section 3.1 reviews the notion of purely inseparable ring extensions, which was introduced by F. Pauer under the name of special algebras. We revisit the characterizations of purely inseparable extensions in terms of the modules of differentials and normal generating sequences given in [49].

Section 3.2 studies purely inseparable extensions in relation to the differential operators and the modules of principal parts. We give a new characterization for purely inseparable ring extensions (Theorem 3.48). More precisely, we prove that a finite ring extension of finite exponent $A \subseteq C$ is purely inseparable if and only if C is projective as $A[C^{p^e}]$-module and $\mathrm{Diff}_A^{p^e}(C)$ is a C-direct summand of $\mathrm{End}_A(C)$ for all $e \geq 0$. Moreover, we re-obtain a characterization in terms of the modules of principal parts from [56], namely, that a finite ring extension of finite exponent $A \subseteq C$ is purely inseparable if and only if $\mathrm{P}_{C/A}^{p^e}$ is a projective C-module for all $e \geq 0$.

Section 3.3 focuses in purely inseparable towers of rings. We first study when an intermediate subring B of a purely inseparable extension $A \subseteq C$ induces a purely inseparable tower $A \subseteq B \subseteq C$. More precisely, we show that this holds if $A \subseteq B$, $B \subseteq C$ and $A \subseteq B[C^{p^e}]$ are $\mathcal{F}$-extensions for all $e \geq 1$ (Proposition 3.54). Later we analyse when the composition of two purely inseparable extensions $A \subseteq B$ and $B \subseteq C$ induces a purely inseparable tower $A \subseteq B \subseteq C$. Among other results, we prove that this happens if $A \subseteq B[C^{p^e}]$ is an $\mathcal{F}$-extension for all $e \geq 1$ (Corollary 3.62).

3.1. Purely inseparable extensions of rings as special algebras

In this section, all the rings are assumed to be of prime characteristic p. This section is mainly expository and follows the original approach from F. Pauer in [49] to analyse the notion of purely inseparable extensions. In Subsection 3.1.1, we study the notion of (generalized) normal generating sequences for finite extensions with finite exponent between local rings. In Subsection 3.1.2, we review the original equivalences that defined purely inseparable ring extensions as special algebras.

3.1.1. (Generalized) normal generating sequences

In this subsection, we give a brief review on the notions of generalized normal generating sequence and normal generating sequences for finite extensions with finite exponent between local rings, which were studied in detail by F. Pauer in [49].

3.1. *Minimal number of generators.* Let $A \subseteq C$ be a finite extension of local rings with finite exponent. Recall that the A-algebras $C^{[e]}$ with $e \geq 0$ are also finite, as we noted in discussion 2.4. For each integer $e \geq 0$, we denote

$$n(e) := \text{minimum number of generators of } C^{[e]} \text{ as } A\text{-algebra.}$$

Note that this number coincides with the minimum number of generators of the $C^{[e]}$-module $\Omega_{C^{[e]}/A}$ by Lemma 2.52. In addition, using the equality $\Omega_{C^{[e]}/A} = \Omega_{C^{[e]}/C^{[e+1]}}$, we see that the number $n(e)$ is also the minimal number of generators for $C^{[e]}$ as $C^{[e+1]}$-algebra. It is clear that there are inequalities

$$n(0) \geq n(1) \geq n(2) \geq \cdots \geq n(e) \geq n(e+1) \geq \cdots .$$

Moreover, for $e \geq \exp(C/A)$, we have $C^{[e]} = A$, so $n(e) = 0$. While, for $0 \leq e < \exp(C/A)$, we have $n(e) > 0$.

We introduce first the notion of generalized normal generating sequence. We will show that one can always choose such a sequence for a finite extension of local rings with finite exponent.

Definition 3.2. Let $A \subseteq C$ be a finite extension of local rings with finite exponent. A sequence of elements $x_1, \ldots, x_n \in C$ is a *generalized normal generating sequence* (GNGS) for C over A if $x_1^{p^e}, \ldots, x_{n(e)}^{p^e}$ is a minimal generating set for $C^{[e]}$ as A-algebra, for all $0 \leq e < \exp(C/A)$.

By convention, the empty set is the only GNGS, where $n = 0$, for a trivial extension $A = C$. The results in this section hold immediately for trivial extensions. Hence, in the subsequent proofs we assume the extensions to have positive exponent to avoid trivialities.

Remark 3.3. In the setting described above, let $d^{[e]} \colon C^{[e]} \to \Omega_{C^{[e]}/A}$ be the universal derivation for each $e \geq 0$. Equivalently, a sequence $x_1, \ldots, x_n \in C$ is a GNGS for C over A if $d^{[e]}x_1^{p^e}, \ldots, d^{[e]}x_{n(e)}^{p^e}$ is a minimal generating set for $\Omega_{C^{[e]}/A}$ as $C^{[e]}$-module for all $0 \leq e < \exp(C/A)$, by Lemma 2.52.

Remark 3.4. The order of the elements of a GNGS matters. Let A be a ring and consider the extension $C = A[X,Y]/\langle X^{p^2}, Y^p\rangle$. Let x, y be the classes of X, Y in C. Then $C = A[x,y]$, $C^{[1]} = A[x^p]$ and $C^{[2]} = A$. Thus, x, y is a GNGS whilst y, x is not.

Lemma 3.5. *Let $A \subseteq C$ be a finite extension of local rings with finite exponent. Any minimal generating set of C as A-algebra contains a GNGS.*

Proof. We proceed inductively on $\exp(C/A)$. Let $\{x_1, \ldots, x_n\} \subset C$ be any minimal generating set for C as A-algebra. If $\exp(C/A) = 1$, then we are done. If $\exp(C/A) > 1$, then $x_1^p, \ldots, x_n^p$ generate $C^{[1]}$ as A-algebra. After rearrangement, we may assume that the first $x_1^p, \ldots, x_{n(1)}^p$ form a minimal generating set. If $\exp(C/A) = 2$, then we are done. In other case, we repeat the process. We continue in this way until the process stops since $A \subseteq C$ has finite exponent. □

3.6. *Sequence of normal exponents.* Let $A \subseteq C$ be a finite extension of local rings with finite exponent. We set $n := n(0)$ for the minimal number of generators for C as A-algebra, as in discussion 3.1. For each $i = 1, \ldots, n$ we denote by $e(i)$ the smallest non-negative integer e such that $n(e) < i$. Equivalently, we have

$$n(e(i)) < i \leq n(e(i) - 1). \tag{3.6.1}$$

It is clear that $\exp(C/A) = e(1) \geq e(2) \geq \cdots \geq e(n) \geq 1$. We define $e(1), \ldots, e(n)$ to be the *sequence of normal exponents* of the extension $A \subseteq C$. We observe that the sequence of minimal number of generators $n(0) \geq n(1) \geq \cdots$ can be recovered from this sequence of normal exponents $e(1), \ldots, e(n)$ via the formula

$$n(e) = \max\{i : e(i) > e\}.$$

If $A = C$, then $n(e) = 0$ for all $e \geq 0$ and the sequence of normal exponents is considered to be empty.

Remark 3.7. For a finite extension of local rings $A \subset C$ with finite exponent, let $x_1, \ldots, x_n \in C$ be a GNGS, which exists by Lemma 3.5. Then, for each normal exponent $e(i)$, where $i = 1, \ldots, n$, we have

$$x_i^{p^{e(i)}} \in A[x_1^{p^{e(i)}}, \ldots, x_{i-1}^{p^{e(i)}}] = A[x_1^{p^{e(i)}}, \ldots, x_{n(e(i))}^{p^{e(i)}}] = C^{[e]}.$$

Thus, we have relations

$$x_i^{p^{e(i)}} = P_i\left(x_1^{p^{e(i)}}, \ldots, x_{n(e(i))}^{p^{e(i)}}\right) \quad i = 1, \ldots, n$$

for some polynomials $P_i \in A[Y_1, \ldots, Y_{n(e(i))}]$, which may be assumed to have degree lower than $p^{e(j)-e(i)}$ in the variable Y_j. Using the above relations for $i = 1, \ldots, n$, we obtain a surjective homomorphism of A-algebras

$$A[X_1, \ldots, X_n] / \left\langle X_i^{p^{e(i)}} - P_i\left(X_1^{p^{e(i)}}, \ldots, X_{n(e(i))}^{p^{e(i)}}\right) : i = 1, \ldots, n \right\rangle \to C, \quad X_i \mapsto x_i. \tag{3.7.1}$$

Remark 3.8. In the previous setting, note that the sum of the numbers $e(i)$ from the sequence of normal exponents coincides with the sum of the minimal numbers of generators $n(e)$, i.e.,

$$n(0) + n(1) + \cdots = e(1) + e(2) + \cdots + e(n). \tag{3.8.1}$$

In fact, given $x_1, \ldots, x_n$ a GNGS for C over A, which exists by Lemma 3.5, then for each $0 \leq e \leq \exp(C/A)$, the sequence $x_1^{p^e}, \ldots, x_{n(e)}^{p^e}$ is a GNGS for $C^{[e]}$ over A. Note that $n(e)$ counts the number of times that the indexes $n(e-1)+1, \ldots, n(e)$ appear on those GNGS of the intermediate subalgebras and that the index i appears on those GNGS exactly $e(i)$ times.

We recall now the concept of normal generating sequence, which might be seen as a possible generalization of the notion of p-basis to higher exponent extensions. It was firstly introduced by R. Rasala for purely inseparable field extensions in [54], where he reviewed the results from G. Pickert ([51]) on the structure equations for these extensions. Then the notion of normal generating sequence was generalized by F. Pauer to the setting of finite ring extensions of finite exponent.

Definition 3.9 ([49, Definition 2.1.5]). Let $A \subseteq C$ be a finite extension of finite exponent. A sequence of elements $x_1, \ldots, x_n \in C$ is a *normal generating sequence* (NGS) for C over A if there are positive integers $e_1 \geq \cdots \geq e_n$ and polynomials $P_i \in A[X_1, \ldots, X_{i-1}]$ for $i = 1, \ldots, n$, such that C admits a presentation $C = A[x_1, \ldots, x_n]$ whose defining relations are $x_i^{p^{e_i}} = P_i(x_1^{p^{e_i}}, \ldots, x_{i-1}^{p^{e_i}})$ for $i = 1, \ldots, n$.

By convention, we will agree the empty set to be the only NGS for any trivial extension, $A = C$. In the setting of finite extensions of local rings with finite exponent, the next proposition shows that a GNGS is indeed a NGS if the intermediate subextensions in discussion 2.4 have a p-basis. Furthermore, in a more general setting, this result will imply that a non-trivial finite ring extension $A \subseteq C$ of finite exponent such that $C^{[e+1]} \subseteq C^{[e]}$ is Galois for all $e \geq 0$, always has a NGS locally at any prime ideal.

Proposition 3.10. *Let $A \subseteq C$ be a finite extension of local rings with finite exponent and let $x_1, \ldots, x_n$ be a GNGS for C over A. If the extension $C^{[e+1]} \subseteq C^{[e]}$ has a p-basis for each $0 \leq e \leq \exp(C/A)$, then the map in (3.7.1) is an isomorphism, and therefore $x_1, \ldots, x_n$ is a NGS for C over A.*

Proof. We use the observations from Remark 3.7. We first note that the ring

$$A[X_1, \ldots, X_n] / \left\langle X_i^{p^{e(i)}} - P_i\left(X_1^{p^{e(i)}}, \ldots, X_{n(e(i))}^{p^{e(i)}}\right) : i = 1, \ldots, n \right\rangle$$

on the left of (3.7.1) is a free A-module of finite rank. In fact, the classes of the monomials $X_1^{\alpha_1} \cdot \ldots \cdot X_n^{\alpha_n}$ with $0 \leq \alpha_i < p^{e(i)}$ form a basis for this ring as A-module. In particular, this implies that its rank is $p^{e(1)+\cdots+e(n)}$. We show now that C is also free and has the same rank.

Since $x_1, \ldots, x_n$ is a GNGS for C over A, we know that the elements $x_1^{p^e}, \ldots, x_{n(e)}^{p^e}$ form a minimal generating set for $C^{[e]}$ as $C^{[e+1]}$-algebra for each $0 \leq e < \exp(C/A)$. Since $C^{[e+1]} \subset C^{[e]}$ has a p-basis, it follows by Corollary 2.54 that $x_1^{p^e}, \ldots, x_{n(e)}^{p^e}$ is a p-basis for $C^{[e]}$ over $C^{[e+1]}$. In particular, $C^{[e]}$ is a free $C^{[e+1]}$-module of rank $p^{n(e)}$ as we noted in Remark 2.23. Using that

$$A \subseteq C^{[\exp(C/A)-1]} \subseteq \ldots \subseteq C^{[e+1]} \subseteq C^{[e]} \subseteq \ldots \subseteq C^{[1]} \subseteq C,$$

we deduce that C is a free A-module of rank $p^{n(1)+\cdots+n(\exp(C/A)-1)}$. Recall from discussion 3.1 that $n(e) = 0$ for $e \geq \exp(C/A)$. Thus, we have

$$n(0) + n(1) + \ldots + n(\exp(C/A) - 1) = e(1) + \ldots + e(n)$$

by Remark 3.8, and so C has rank $p^{e(1)+\cdots+e(n)}$. Finally, we have shown that the map in (3.7.1) is a surjective homomorphism between free A-modules of the same rank, so it must be an isomorphism and it is clear that $x_1, \ldots, x_n$ is a NGS for C over A. □

3.1.2. On purely inseparable extensions of rings

We begin this subsection with one of the equivalent conditions that F. Pauer ([49]) used to define the notion of *special algebra*. We take it as our definition of purely inseparable extension of rings and we show the equivalent characterizations.

Definition 3.11. A finite ring extension $A \subseteq C$ is *purely inseparable* if the following conditions hold

(i) $A \subseteq C$ has finite exponent,

(ii) C is a projective A-module, and

(iii) for each prime ideal $\mathfrak{p} \subset A$, there is a faithfully flat extension $A_{\mathfrak{p}} \to A'$ such that $C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A'$ is isomorphic to an A'-algebra $A'[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$ for some $n \geq 0$ and $e_i > 0$.

Note that any trivial extension of rings, $A = C$, is considered a purely inseparable extension of exponent zero.

Remark 3.12. Observe that condition (i) in the above definition implies $\exp(C_{\mathfrak{p}}/A_{\mathfrak{p}}) \leq \exp(C/A)$ for every prime ideal $\mathfrak{p} \subset A$ by Lemma 2.10. Moreover, using Lemma 2.9 and the presentations from condition (iii), we see that $\exp(C_{\mathfrak{p}}/A_{\mathfrak{p}})$ coincides with the exponent of the corresponding extension $A' \subset C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A'$.

Remark 3.13. Note that condition (ii) in the definition of purely inseparable extension can be replaced by the condition that C is an A-module of finite presentation as a consequence of Proposition 1.7. In particular, the A-algebra C has finite presentation (see discussion A.40). In fact, C is a flat A-module as condition (iii) already implies that $C_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module for all prime ideal $\mathfrak{p} \subset A$. This follows from Proposition A.15.(2) and the fact that $A_{\mathfrak{p}} \to A'$ is a faithfully flat ring extension and $C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A'$ is a free A'-module, in particular, flat.

Example 3.14. Any finite extension of fields $K \subseteq L$ with finite exponent is purely inseparable. In fact, let $\overline{K}$ be an algebraic closure of K. Then $K \to \overline{K}$ is faithfully flat and $L \otimes_K \overline{K} \cong \overline{K}[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$ for some $e_i > 0$ (see [54]).

We give another example of a particular class of purely inseparable extensions, called *modular extensions with splitting p-basis*. These extensions will be studied later with more detail in Subsection 4.1.3 from the last chapter.

Example 3.15. Let A be a ring and let $e_1 \geq \cdots \geq e_n$ be positive integers. We consider the A-algebra

$$C := A[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle.$$

Then the classes of $X_1, \ldots, X_n$ form a NGS for C over A and we can write $C = A[x_1, \ldots, x_n]$ with defining relations $x_1^{p^{e_1}} = \cdots = x_n^{p^{e_n}} = 0$. We claim that $A \subset C$ is a purely inseparable extension. In fact, it is clear that C has finite exponent over A, more precisely $\exp(C/A) = e_1$. Note also that C is a finite free A-module with basis $\{x_1^{\alpha_1} \cdot \ldots x_n^{\alpha_n} : 0 \leq \alpha_i < e_i\}$. In particular, $A \subset C$ is a finite extension such that C is projective as A-module. In addition, observe that C is a local ring with maximal ideal $\langle x_1, \ldots, x_n \rangle$ and that the presentation for C as A-algebra is as the one that appears in the definition of purely inseparable extension. Similarly, we see that $A \subset C^{[e]}$ is

also purely inseparable of exponent $e_1 - e$ for all $1 \leq e < \exp(C/A)$. Indeed, $n(e)$ coincides with the largest positive integer $m \leq n$ such that $x_m^{p^e} \neq 0$ and then

$$C^{[e]} = A[x_1^{p^e}, \ldots, x_{n(e)}^{p^e}]$$

and the defining relations for this A-algebra are $(x_1^{p^e})^{p^{e_1-e}} = \ldots = (x_{n(e)}^{p^e})^{p^{e_{n(e)}-e}} = 0$. Furthermore, it follows that $C^{[e+1]} \subset C^{[e]}$ is a Galois extension of exponent one and with p-basis $x_1^{p^e}, \ldots, x_{n(e)}^{p^e}$.

The above example motivates the next proposition for purely inseparable ring extensions in general.

Proposition 3.16. *Let $A \subseteq C$ be a finite ring extension of finite exponent. If $A \subseteq C$ is a purely inseparable extension, then $C^{[e+1]} \subset C^{[e]}$ is a Galois extension for all $0 \leq e < \exp(C/A)$.*

Proof. We proceed by induction on $\exp(C/A)$. We have nothing to prove in the trivial case. The exponent one case is true since purely inseparable extensions of exponent one and Galois extensions are the same (see Theorem 2.71).

Assume now that $\exp(C/A) > 1$. Note that $A \subset C^{[1]}$ is a finite extension of exponent $\exp(C/A) - 1$. If this extension were purely inseparable, we could apply the inductive hypothesis to deduce that the extension $(C^{[1]})^{[e+1]} \subset (C^{[1]})^{[e]}$ is Galois for all $0 \leq e < \exp(C/A) - 1$. Since $(C^{[1]})^{[e]} = C^{[e+1]}$, this would imply that $C^{[e+1]} \subset C^{[e]}$ is Galois for $1 \leq e < \exp(C/A)$. If $C^{[1]} \subset C$ were Galois, the result would hold. Thus, we prove that $A \subset C^{[1]}$ is purely inseparable and $C^{[1]} \subset C$ is Galois.

Let $\mathfrak{p} \subset A$ be any prime ideal. Since $A \subset C$ is purely inseparable, there is a faithfully flat homomorphism of rings $A_\mathfrak{p} \to A'$ such that $C' := C_\mathfrak{p} \otimes_{A_\mathfrak{p}} A'$ is of the form $A'[x_1, \ldots, x_n]$ with defining relations $x_1^{p^{e_1}} = \cdots = x_n^{p^{e_n}} = 0$ for certain $e_1 \geq \cdots \geq e_n \geq 1$. Since $A_\mathfrak{p} \to A'$ is in particular flat, we have by Lemma 2.6 that

$$C'^{[1]} = C_\mathfrak{p}^{[1]} \otimes_{A_\mathfrak{p}} A',$$

Thus, we have that $C'^{[1]} = A'[x_1^p, \ldots, x_{n(1)}^p]$ with defining relations

$$(x_1^{p^e})^{p^{e_1-e}} = \ldots = (x_{n(e)}^{p^e})^{p^{e_{n(e)}-e}} = 0$$

and that $\{x_1, \ldots, x_n\}$ is a p-basis for C' over $C'^{[1]}$, as we noted in Example 3.15. Moreover, since $C_\mathfrak{p}^{[1]} \subset C_\mathfrak{p}$ is a finite extension of local rings and $A_\mathfrak{p} \to A'$ is faithfully flat, we deduce that $C_\mathfrak{p}$ has a p-basis over $C_\mathfrak{p}^{[1]}$ by Lemma 2.69.

Hence, it only lefts to show that $C^{[1]}$ is a projective A-module and that C is a projective $C^{[1]}$-module to conclude that $A \subset C^{[1]}$ is purely inseparable and $C^{[1]} \subset C$ is Galois. Since $A \subset C$ is purely inseparable, we already know that C is a finite projective A-module. Then $C^{[1]}$ is also finite over A (see discussion 2.4). In addition, since $C_\mathfrak{p}$ has a p-basis over $C_\mathfrak{p}^{[1]}$, in particular, $C_\mathfrak{p}$ is a flat $C_\mathfrak{p}^{[1]}$-module. This holds for any prime ideal $\mathfrak{p} \subset A$, so C is a flat $C^{[1]}$-module by Proposition A.13. Therefore, by Lemma 1.18, we conclude that C is projective as $C^{[1]}$-module and this completes the proof. □

We will show that the converse of this proposition is also true. The proof will involve the next result that ensures that an extension is purely inseparable if it has a NGS locally at any prime ideal (see Definition 3.9).

Proposition 3.17. *Let $A \subseteq C$ be a finite ring extension of finite exponent such that C is projective as A-module. If the extension $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}}$ has a NGS for each prime ideal $\mathfrak{p} \subset A$, then $A \subseteq C$ is purely inseparable.*

Proof. Since $A \subseteq C$ is a finite ring extension of finite exponent and C is projective as A-module, we only have to check that for each prime ideal $\mathfrak{p} \subset A$, there is a faithfully flat extension $A_{\mathfrak{p}} \to A'$ such that $C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A'$ is isomorphic to an A'-algebra of the form $A'[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$ with $n \geq 0$ and $e_i > 0$.

Let $\mathfrak{p} \subset A$ be a prime ideal and let $x_1, \ldots, x_n \in C_{\mathfrak{p}}$ be a NGS for $C_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$. Then there are positive integers $e_1 \geq \cdots \geq e_n$ and polynomials $P_i \in A_{\mathfrak{p}}[X_1, \ldots, X_{i-1}]$ for $i = 1, \ldots, n$, such that $C_{\mathfrak{p}} = A_{\mathfrak{p}}[x_1, \ldots, x_n]$ where the defining relations are given by $x_i^{p^{e_i}} = P_i(x_1^{p^{e_i}}, \ldots, x_{i-1}^{p^{e_i}})$. We can write each polynomial as

$$P_i(X_1, \ldots, X_{i-1}) = \sum_{\alpha \in \mathcal{A}_i} a_{i,\alpha} X_1^{\alpha_1} \cdots X_{i-1}^{\alpha_{i-1}},$$

for a finite set of exponents $\mathcal{A}_i \subset \mathbb{N}_0^{i-1}$. We define the $A_{\mathfrak{p}}$-algebra

$$A' := A_{\mathfrak{p}}[z_{i,\alpha} : \alpha \in \mathcal{A}_i, i = 1, \ldots, n]$$

with relations $z_{i,\alpha}^{p^{e_i}} = a_{i,\alpha}$. Note that A' is a local ring and that it is a free $A_{\mathfrak{p}}$-module with basis the monomials on $z_{i,\alpha}$ with exponent β such that $0 \leq \beta_{i,\alpha} < p^{e_i}$. Therefore, A' is a faithfully flat $A_{\mathfrak{p}}$-algebra. Note that $C' := C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A'$ has a presentation $C' = A_{\mathfrak{p}}[x_1, \ldots, x_n]$ with relations

$$x_i^{p^{e_i}} = \sum_{\alpha \in \mathcal{A}_i} z_{i,\alpha}^{p^{e_i}} (x_1^{p^{e_i}})^{\alpha_1} \cdots (x_{i-1}^{p^{e_i}})^{\alpha_{i-1}},$$

as A'-algebra. We define $y_i := x_i - \sum_{\alpha \in \mathcal{A}_i} a_{i,\alpha} x_1^{\alpha_1} \cdots x_{i-1}^{\alpha_{i-1}}$. Then $C' = A'[y_1, \ldots, y_n]$, and the defining relations are exactly $y_i^{p^{e_i}} = 0$. This completes the proof that $A \subseteq C$ is purely inseparable. □

Using the results presented throughout this section, we recover the original characterization of special algebras given by F. Pauer. That is, the next theorem collects some equivalences for a finite ring extension of finite exponent to be purely inseparable. It extends in some sense the equivalences (1) ⇔ (2) ⇔ (4) from Theorem 2.71 for exponent one extensions to the higher exponent setting.

Theorem 3.18 ([49, Satz 2.2.5])**.** *Let $A \subseteq C$ be a finite ring extension of finite exponent. Then the following conditions are equivalent:*

(1) $A \subseteq C$ is purely inseparable.

(2) $C^{[e+1]} \subset C^{[e]}$ is a Galois extension for all $0 \leq e < \exp(C/A)$.

(3) $\Omega_{C^{[e]}/A}$ *is a projective* $C^{[e]}$*-module for all* $0 \leq e < \exp(C/A)$.

(4) C *is a projective* A*-module and for each prime ideal* $\mathfrak{p} \subset A$*, the* $C_{\mathfrak{p}}$ *has a NGS over* $A_{\mathfrak{p}}$.

Proof. The implication (1)⇒(2) is Proposition 3.16. The equivalence (2)⇔(3) follows directly from Proposition 2.55. It is clear that (2)⇒(4) by Proposition 3.10. Finally, (4)⇒(1) is Proposition 3.17. □

As a direct consequence of the equivalence (1)⇔(2) in the above theorem, we obtain two useful properties of purely inseparable ring extensions. In the first place, the equivalence implies that for a finite ring extension of finite exponent to purely inseparable can be checked inductively.

Corollary 3.19. *Let* $A \subseteq C$ *be a finite ring extension of finite exponent. Then* $A \subseteq C$ *is purely inseparable if and only if* $A \subseteq C^{[1]}$ *is purely inseparable and* $C^{[1]} \subseteq C$ *is Galois.*

Proof. The results follows from the fact that $(C^{[1]})^{[e]} = A[(C^{[1]})^{p^e}] = A[C^{p^{e+1}}] = C^{[e+1]}$ for all $e \geq 0$ and the equivalence (1)⇔(2) in Theorem 3.18. □

In the second place, we see that purely inseparable extensions behave well under base change and faithfully flat descent. The proof of next proposition relies on the fact that purely inseparable extensions inherit this well behaviour from Galois extensions (see Lemma 2.45.(2) and Proposition 2.70).

Proposition 3.20. *Let* $A \subseteq C$ *be a finite ring extension and let* $A \to A'$ *be an homomorphism of rings. Denote* $C' := C \otimes_A A'$.

(1) If $A \subseteq C$ *is purely inseparable, then* $A' \subseteq C'$ *is also purely inseparable of the same exponent.*

(2) If $A \to A'$ *is faithfully flat and* $A' \subseteq C'$ *is purely inseparable, then* $A \subseteq C$ *is also purely inseparable of the same exponent.*

Proof. The result is trivial if $A = C$, so we assume that $\exp(C/A) \geq 1$. Since $A \subset C$ is a finite extension such that C is projective as A-module, we have also that $A' \subseteq C'$ is a finite extension such that C' is projective as A'-module, as we noted in Remark 1.16.

We assume first that $A \subset C$ is purely inseparable. Then $C^{[e+1]} \subset C^{[e]}$ is an exponent one Galois extension for all $0 \leq e < \exp(C/A)$ by Theorem 3.18. In particular, $C^{[e]}$ is a flat $C^{[e+1]}$-module. Hence, by Lemma 2.45.(2) we have that $C^{[e+1]} \otimes_A A' \subset C^{[e]} \otimes_A A'$ is also an exponent one Galois extension. By Lemma 2.6, we know that $C^{[e]} \otimes_A A' = C'^{[e]}$ for all $e \geq 0$. In particular, $C'^{[e]} = A$ for all $e \geq \exp(C/A)$. Then it is clear that $C'^{[e+1]} \subset C'^{[e]}$ is Galois and has exponent one. Hence, $\exp(C'/A') = \exp(C/A)$. Using the equivalence (1)⇔(2) from Theorem 3.18, we conclude that $A' \subset C'$ is purely inseparable.

We assume now that $A \to A'$ is faithfully flat and that $A' \subset C'$ is purely inseparable. Then $C'^{[e+1]} \subset C'^{[e]}$ is Galois for all $0 \leq e < \exp(C'/A')$. Since $A \to A'$ is in particular flat, we have that $C'^{[e]} = C^{[e]} \otimes_A A'$ for all $e \geq 0$ by Lemma 2.6. Thus, $C^{[e+1]} \otimes_A A' \subset C^{[e]} \otimes_A A'$ is Galois. Since being Galois descends by faithfully flat morphisms (see Proposition 2.70), we deduce that $C^{[e]} \subset C^{[e+1]}$ is Galois for all $0 \leq e < \exp(C'/A')$. By Lemma 2.9, we know that $\exp(C'/A') = \exp(C/A)$. Therefore, using again the equivalence (1)⇔(2) from Theorem 3.18, we conclude that $A \subset C$ is purely inseparable. □

We end this section with another characterization from F. Pauer for purely inseparable extensions that describes these extensions as flat families of purely inseparable extensions. We have seen in the exponent one case that a finite extension $A \subseteq C$ is Galois if and only if C is projective as A-module and for each maximal ideal $\mathfrak{m} \subset A$ the extension $A/\mathfrak{m} \subseteq C/\mathfrak{m}C$ is Galois (see Corollary 2.49). However, this characterization must be refined for purely inseparable extensions of higher exponent. The key is to ensure that for all $e \geq 0$, we have $C^{[e]} \otimes_A A/\mathfrak{m} = (C/\mathfrak{m}C)^{[e]}$ for every maximal ideal $\mathfrak{m} \subset A$.

With this aim, we introduce in the next definition a class of extensions that satisfies the mentioned condition. It will be particularly useful in the study of purely inseparable towers of rings in Section 3.3 from this chapter.

Definition 3.21. A finite ring extension $A \subseteq C$ of finite exponent is an *$\mathcal{F}$-extension* if $C^{[e]}$ is a projective $C^{[e+1]}$-module for all $e \geq 0$.

Remark 3.22. Note that if $A \subseteq C$ is an $\mathcal{F}$-extension, then $A \subseteq C^{[e]}$ is also an $\mathcal{F}$-extension for all $e \geq 0$, because $(C^{[e]})^{[k]} = C^{[e+k]}$ for any integer $k \geq 0$.

Remark 3.23. Let $A \subseteq C$ be an $\mathcal{F}$-extension. Let $A \to A'$ be any homomorphism of rings and denote $C' := C \otimes_A A'$. Then $A' \subseteq C'$ is also an $\mathcal{F}$-extension. In particular, C is projective as A-module and so $A' \subseteq C'$ is also a finite projective ring extension (Remark 1.16). The extension $A' \subseteq C'$ has finite exponent $\exp(C'/A') \leq \exp(C/A)$ by Lemma 2.8. We also know that $C^{[e]} \otimes_A A' = C'^{[e]}$ for all $e \geq 0$ by Lemma 2.6. Since being projective is stable under base change (Proposition 1.4.(1)), it follows that $C'^{[e]}$ is also projective as $C'^{[e+1]}$-module and, therefore, $A' \subset C'$ is also an $\mathcal{F}$-extension.

Lemma 3.24. *Let $A \subseteq C$ be a finite ring extension of finite exponent. Then $A \subseteq C$ is an $\mathcal{F}$-extension if and only if C is a projective $C^{[e]}$-module for all $e \geq 0$. In this case, $C^{[e]}$ is also a projective A-module for all $e \geq 0$.*

Proof. If $A \subseteq C$ is an $\mathcal{F}$-extension, then $C^{[e]}$ is a projective $C^{[e+1]}$-module for all $e \geq 0$. In particular, C is projective as $C^{[1]}$-module. By induction on e, we can assume that C is a projective $C^{[e]}$-module. Then we can apply Proposition 1.5 to the projective ring map $C^{[e+1]} \to C^{[e]}$ and to C as projective $C^{[e]}$-module to deduce that C is projective as $C^{[e+1]}$-module. Since $A \subseteq C$ has finite exponent, the process ends at $e = \exp(C/A)$.

Conversely, if C is a projective $C^{[e]}$-module for all $e \geq 0$. For each e, we can consider C as both a finite projective $C^{[e]}$-module and as a projective $C^{[e+1]}$-module. Then, by Lemma 1.17, we conclude that $C^{[e]}$ is a projective $C^{[e+1]}$-module.

In addition, assume that $A \subseteq C$ is an $\mathcal{F}$-extension. Then we have a tower of rings $A \subseteq C^{[e]} \subseteq C$ for all $e \geq 0$, where C is projective as both a $C^{[e]}$-module and an A-module. Thus, we conclude that $C^{[e]}$ is a projective A-module by Lemma 1.17. □

Finally, we give the characterization of purely inseparable extensions as flat families of purely inseparable extensions using the notion of $\mathcal{F}$-extension.

Theorem 3.25 ([49, Satz 2.2.5]). *Let $A \subseteq C$ be a finite ring extension of finite exponent. Then $A \subseteq C$ is purely inseparable if and only if the following conditions hold:*

(1) $A \subseteq C$ is an $\mathcal{F}$-extension; and

(2) for any maximal ideal $\mathfrak{m} \subset A$, the extension $A/\mathfrak{m} \subseteq C/\mathfrak{m}C$ is purely inseparable.

Proof. If $A = C$, we have nothing to prove and the characterization is true. Hence, we assume $\exp(C/A) \geq 1$. Let $A \subset C$ be purely inseparable. Note that it is an $\mathcal{F}$-extension by the equivalence (1)⇔(2) in Theorem 3.18. Taking the base change by $A \to A/\mathfrak{m}$, we know also that $A/\mathfrak{m} \subset C/\mathfrak{m}C$ is purely inseparable by Proposition 3.20.(1).

Conversely, assume that $A \subset C$ is an $\mathcal{F}$-extension such that $A/\mathfrak{m} \subset C/\mathfrak{m}C$ is purely inseparable for each maximal ideal $\mathfrak{m} \subset A$. Recall that there is a natural homeomorphism $\operatorname{Spec}(C^{[e]}) \simeq \operatorname{Spec}(A)$ for all $e \geq 0$ (Remark 2.2), so we can identify the maximal ideals. By hypothesis, $(C/\mathfrak{m}C)^{[e+1]} \subseteq (C/\mathfrak{m}C)^{[e]}$ is Galois for all $e \geq 0$. Note that

$$(C/\mathfrak{m}C)^{[e]} = (C \otimes_A (A/\mathfrak{m}))^{[e]} = C^{[e]} \otimes_A (A/\mathfrak{m}) = C^{[e]}/\mathfrak{m}C^{[e]}$$

by Lemma 2.6. Therefore, by Corollary 2.49, we have that $C^{[e+1]} \subset C^{[e]}$ is Galois for all $e \geq 0$. Finally, using Theorem 3.18, we conclude that $A \subset C$ is purely inseparable. □

3.2. Purely inseparable extensions of rings and differential operators

This section is dedicated to the study of purely inseparable ring extensions from the perspective of differential operators and modules of principal parts. We reproduce the results from [11, §4] obtained by the author of this thesis in collaboration with D. Sulca. We begin with some preliminaries on differential operators and modules of principal parts (Subsection 3.2.1). Then we focus on the extension of differential operators for finite ring extensions of finite exponent along some Galois intermediate subextensions (Subsection 3.2.2). Finally, we use these properties to prove a new characterization for purely inseparable extensions in terms of differential operators and to re-obtain an already known characterization related to the modules of principal parts (Subsection 3.2.3).

3.2.1. Differential operators and modules of principal parts

We maintain this subsection in the general setting of rings of any characteristic commutative with unity. We give a brief introduction on differential operators and review the construction of the modules of principal parts and the universal differential operator. We refer to [25, §16] for more details. We begin by reviewing some basic and useful properties of the bracket operator for homomorphisms of modules.

3.26. *Bracket operator.* Let C be an A-algebra and let M be a C-module. For any A-linear map $D\colon C \to M$ and for any $x \in C$, we define an A-linear map $[x, D]\colon C \to M$ by the formula

$$[x, D](c) := xD(c) - D(xc) \quad \text{for each } c \in C.$$

Note that for $M = C$, the bracket $[x, D]$ coincides with the bracket defined for $\mathrm{End}_A(C)$ in discussion 1.22.

Lemma 3.27. *Let C be an A-algebra and let M be a C-module. Let $D\colon C \to M$ be an A-linear map. For any $x, y \in C$ and $a \in A$, we have:*

(1) (Linearity) $[ax, D] = a[x, D]$ *and* $[x + y, D] = [x, D] + [y, D]$;

(2) (Symmetry) $[x, [y, D]] = [y, [x, D]]$;

(3) (Decomposition for a product) $[xy, D] = x[y, D] + y[x, D] - [y, [x, D]]$;

(4) (Reduction to generators) Let $S \subseteq C$ be a set and let n be a positive integer. If $[s_0, [s_1, [\ldots, [s_k, D]\ldots]]] = 0$ for any $s_0, \ldots, s_k \in S$, then we have $[f_0, [f_1, [\ldots, [f_k, D]\ldots]]] = 0$ for any $f_0, \ldots, f_k \in A[S]$.

Proof. Note that the linearity of the bracket stated in (1) is straightforward from the definition. We prove properties (2) and (3) by evaluating the expressions at any element in C. For any $x, y, c \in C$, we have

$$[x, [y, D]](c) = x[y, D](c) - [y, D](xc) = xyD(c) - xD(yc) - yD(xc) + D(xyc).$$

Observe that this expression is symmetric in x, y. Thus, $[x, [y, D]] = [y, [x, D]]$ as we wanted. In addition, for any $x, y, c \in C$, we have

$$\begin{aligned}[xy, D](c) &= xyD(c) - D(xyc) = xyD(c) - xD(yc) + xD(yc) - D(xyc)\\ &= x[y, D](c) + [x, D](yc) = x[y, D](c) + y[x, D](c) - [y, [x, D]](c).\end{aligned}$$

Now we prove (4). Let f be a monomial on elements of S, i.e., $f = s_1 \cdot \ldots \cdot s_n$ with $s_i \in S$ not necessarily different. Then we define $\deg f$ to be the minimal integer n such that f admits an expression as before. We note that, using the linearity of the bracket from (1), the affirmation in (4) holds if we prove it for $f_j \in A[S]$ that are monomial expressions on the elements of S. Under this assumption, we proceed by induction on $\deg f_0 + \cdots + \deg f_k$. If $\deg f_0 = \cdots = \deg f_k = 1$, then $[f_0, [f_1, [\ldots, [f_k, D]\ldots]]] = 0$ by hypothesis. Suppose that $\deg f_i > 1$ for some i, then we can assume that $\deg f_0 > 1$ by the symmetry from (2). That is, we can write $f_0 = sg_0$ for some $s \in S$ and some

monomial expression g_0 on S of degree lower than $\deg f_0$. We apply the decomposition from (2) to obtain

$$[f_0,[f_1,[\dots[f_k,D]\dots]]] = s[g_0,[f_1,[\dots[f_k,D]\dots]]] + g_0[s,[f_1,[\dots[f_k,D]\dots]]] - [g_0,[s,[f_1,[\dots[f_k,D]\dots]]]]$$

Note that $\deg g_0 + \deg f_1 + \cdots + \deg f_k$ and $\deg s + \deg f_1 + \cdots + \deg f_k$ are lower than $\deg f_0 + \cdots + \deg f_k$. Thus, all the terms on the right of the equality are zero by the inductive hypothesis. Therefore the left side is also zero, as we wanted. □

The formulas from the next two lemmas will be used later to study the extension of differential operators, especially in the proof of Proposition 3.39 in the following subsection.

Lemma 3.28. *Let C be an A-algebra and let M be a C-module. Then for any A-linear map $D\colon C \to M$ and $x_1,\dots,x_k,c \in C$, we have:*

$$[x_1,[x_2,[\dots,[x_k,D]]]](c) = \sum_{S\subset[k]} (-1)^{k-|S|}\mathbf{x}_S \cdot D(\mathbf{x}_{S^c}c),$$

where $[k] := \{1,\dots,k\}$, $\mathbf{x}_S := \prod_{i\in S} x_i$ and $\mathbf{x}_{S^c} := \prod_{i\notin S} x_i$.

Proof. We prove the formula by induction on k. For $k=1$, it is clear since $[x_1,D](c) = x_1D(c) - D(x_1c)$ by definition. Assume that $k>1$ and recall that $E := [x_k,D]$ is an A-linear map from C to M. Thus, we can apply the inductive hypothesis to $[x_1,[x_2,[\dots,[x_{k-1},E]]]]$ and obtain

$$\begin{aligned}
[x_1,[x_2,[\dots,[x_{k-1},E]]]] &= [x_1,[x_2,\dots,[x_k,D]]](c)\\
&= \sum_{S\subset[k-1]} (-1)^{k-1-|S|}\mathbf{x}_S \cdot [x_k,D](\mathbf{x}_{S^c}\cdot c)\\
&= \sum_{S\subset[k-1]} (-1)^{k-1-|S|}\mathbf{x}_S \cdot (x_kD(\mathbf{x}_{S^c}\cdot c) - D(x_k\mathbf{x}_{S^c}\cdot c))\\
&= \sum_{S\subset[k-1]} (-1)^{k-1-|S|}\mathbf{x}_{S\cup\{k\}} \cdot D(\mathbf{x}_{S^c}\cdot c) + (-1)^{k-|S|}\mathbf{x}_S \cdot D(\mathbf{x}_{S^c\cup\{k\}}\cdot c)\\
&= \sum_{S\subset[k]} (-1)^{k-|S|}\mathbf{x}_S \cdot D(\mathbf{x}_{S^c}c).
\end{aligned}$$

Note that the last equality holds because the first term inside the sum includes the sets $S\subset[k]$ containing k and the second term includes those sets that do not contain k. □

As we show in the following lemma, the previous formula can be refined by grouping the repeated elements x_i that appear inside the bracket.

Lemma 3.29. *Let C be an A-algebra and let M be a C-module. For any A-linear map $D\colon C \to M$ and $x_1, \dots, x_m, c \in C$, we have:*

$$[\underbrace{x_1, [\dots, [x_1}_{r_1}, [\underbrace{x_2, [\dots, [x_2}_{r_2}, [\dots, [\underbrace{x_m, [\dots, [x_m}_{r_m}, D] \dots]] \dots]] \dots]]] \dots]](c)$$
$$= \sum_{\substack{S_i \subset [r_i] \\ i=1,\dots,m}} \prod_{i=1}^{m} \Big((-1)^{r_i - |S_i|} x_i^{|S_i|} D \quad c \cdot \prod_{i=1}^{m} x_i^{r_i - |S_i|} \Big) \Big(\quad$$

where r_i denotes the number of appearances of each x_i on the bracket expression and $[d] := \{1, \dots, d\}$ for any positive integer d.

Proof. Let $k := r_1 + \cdots + r_m$. There is a partition $[k] = A_1 \uplus \cdots \uplus A_m$ where the A_i are disjoint subsets such that $|A_i| = r_i$ for $i = 1, \dots, m$. If we identify each subset A_i with $[r_i]$, then choosing a subset $S \subset [k]$ is equivalent to choosing a collection of subsets $S_i \subset [r_i]$ such that $|S| = |S_1| + \cdots + |S_m|$. Then, using the formula from Lemma 3.28, the first expression on the statement can be expressed as

$$\sum_{S \subset [k]} \Big((-1)^{k-|S|} \mathbf{x}_S \cdot D(\mathbf{x}_{S^c} c) = \sum_{\substack{S_i \subset [r_i] \\ i=1,\dots,m}} \prod_{i=1}^{m} (-1)^{r_i - |S_i|} x_i^{|S_i|} D \quad c \cdot \prod_{i=1}^{m} x_i^{r_i - |S_i|} \Big) \Big(\quad$$

where the last equality follows from the use of the partition of $[k]$ and from observing that $\mathbf{x}_S = x_1^{\alpha_1} \cdot \dots \cdot x_k^{\alpha_k}$ and $\mathbf{x}_{S^c} = x_1^{r_1 - \alpha_1} \cdot \dots \cdot x_k^{r_k - \alpha_k}$ for some $0 \leq \alpha_i \leq r_i$. In fact, $\alpha_i = |S_i|$. □

Now, we introduce differential operators, the modules of principal parts and some basic properties of both.

3.30. *Differential operators.* Let C be an A-algebra and let M be a C-module. An homomorphism of A-modules $D\colon C \to M$ is an *A-differential operator from C to M* if there exists a non-negative integer k such that

$$[x_0, [x_1, [\dots, [x_k, D] \dots]]] = 0 \quad \text{in } \mathrm{Hom}_A(C, M) \text{ for all } x_0, \dots, x_k \in C. \tag{3.30.1}$$

The smallest integer k with this property is *the order* of the differential operator D. We denote by $\mathrm{Diff}_A^k(C, M)$ the set of A-differential operators from C to M of order at most k, which is a C-submodule of the left C-module $\mathrm{Hom}_A(C, M)$. Note that the construction of $\mathrm{Diff}_A^k(C, M)$ is functorial in M. We make some additional observations:

(1) The A-differential operators of order zero are just the C-linear maps $D\colon C \to M$. In fact, for any $D \in \mathrm{Hom}_A(C, M)$ and $x \in C$, we have

$$[x, D] = 0 \quad \Leftrightarrow \quad xD(c) = D(xc) \quad \text{for all } c \in C \quad \Leftrightarrow \quad D \in \mathrm{Hom}_C(C, M).$$

Since any C-linear map $D\colon C \to M$ is uniquely determined by $D(1) \in M$, we have a natural identification $\mathrm{Diff}_A^0(C, M) = \mathrm{Hom}_C(C, M) \simeq M$ given by $D \mapsto D(1)$.

(2) There is a filtration

$$M \simeq \mathrm{Hom}_C(C, M) = \mathrm{Diff}^0_A(C, M) \subseteq \mathrm{Diff}^1_A(C, M) \subseteq \cdots \subseteq \mathrm{Hom}_A(C, M),$$

of the left C-module $\mathrm{Hom}_A(C, M)$ that is not exhaustive in general. The *module of A-differential operators from C to M* is $\mathrm{Diff}_A(C, M) = \cup_{n=0}^{\infty} \mathrm{Diff}^n_A(C, M)$.

(3) We can check the order of differential operators recursively. That is, $D \in \mathrm{Diff}^n_A(C, M)$ if and only if $[x, D] \in \mathrm{Diff}^{n-1}_A(C, M)$ for all $x \in C$.

(4) The C-module of derivations $\mathrm{Der}_A(C, M)$ coincides with the submodule of differential operators $D \in \mathrm{Diff}^1_A(C, M)$ such that $D(1) = 0$. In fact, combining (1) and (3), we have that $D \in \mathrm{Diff}^1_A(C, M)$ if and only if $[x, D] \in \mathrm{Hom}_C(C, M)$ for all $x \in C$. This is the same as $[x, D](c) = c[x, D](1)$ for all $x, c \in C$, equivalently, this condition can be expressed as

$$xD(c) - D(xc) = cxD(1) - cD(x).$$

If $D(1) = 0$, then the above condition coincides with the Leibniz rule $D(xc) = xD(c) + cD(x)$.

(5) Given an element $m \in M$ and a A-differential operator $D\colon C \to C$ of order at most k, we define a map $(m \cdot D)\colon C \to M$ as the composition of D and right multiplication by m, i.e, $(m \cdot D)(c) = D(c)m$. This map is also an A-differential operator of order at most k.

(6) From (4), we deduce that any A-differential operator of order at most 1 can be written uniquely as a sum of a differential operator of order 0 and an A-derivation. That is, we have a decomposition into a direct sum of C-submodules

$$\mathrm{Diff}^1_A(C, M) = M \oplus \mathrm{Der}_A(C, M), \quad D = D(1) + (D - D(1)).$$

When $M = C$, we simply write $\mathrm{Diff}_A(C) = \mathrm{Diff}_A(C, C)$ and $\mathrm{Diff}^k_A(C) = \mathrm{Diff}^k_A(C, C)$ for all $k \geq 0$.

3.31. *Modules of principal parts.* We consider now the A-algebra $C \otimes_A C$ with the natural structure of left C-module. Let J be the kernel of the multiplication map $C \otimes_A C \to C$ as in discussion 2.12. For each integer $k \geq 0$, we set the quotient C-module

$$\mathrm{P}^k_{C/A} := (C \otimes_A C)/J^{k+1}$$

with the structure induced by the left C-module structure of $C \otimes_A C$. The C-module $\mathrm{P}^k_{C/A}$ is the *module of principal parts* of order k of C relative to A and the *universal A-differential operator* of order k is given by the map

$$\delta_k\colon C \to \mathrm{P}^k_{C/A}, \quad x \mapsto \overline{1 \otimes x},$$

We note that δ_k is an A-differential operator of order k satisfying the following universal property:

Proposition 3.32 ([25, Proposition 16.8.4]). *Let C be an A-algebra and let M be a C-module. Then for any A-differential operator $D\colon C \to M$ of order at most k, there is only one C-linear map $\varphi\colon \mathrm{P}^k_{C/A} \to C$ such that $D = \varphi \circ \delta_k$. Equivalently, there is an isomorphism of C-modules*

$$\mathrm{Hom}_C(\mathrm{P}^k_{C/A}, M) \to \mathrm{Diff}^k_A(C, M), \quad \varphi \mapsto \varphi \circ \delta_k$$

We recall some useful properties of the modules of principal parts. First, we see that finiteness conditions for C as an A-algebra induce good finiteness properties in the C-modules of principal parts $\mathrm{P}^k_{C/A}$.

Proposition 3.33 ([25, Proposition 16.3.9 and Corollaire 16.4.22]). *Let C be an A-algebra.*

(1) If C is finitely generated as an A-algebra, then $\mathrm{P}^k_{C/A}$ is finitely generated as C-module.

(2) If C has finite presentation as an A-algebra, then $\mathrm{P}^k_{C/A}$ is a C-module of finite presentation.

We review now the good behaviour of the modules of principal parts with base change.

Proposition 3.34 ([25, Proposition 16.4.5]). *Let C be an A-algebra and let $A \to A'$ be any homomorphism of rings. Let $C' := C \otimes_A A'$. Then there is a natural isomorphism*

$$\mathrm{P}^k_{C'/A'} = C' \otimes_C \mathrm{P}^k_{C/A} \tag{3.34.1}$$

In particular, if $S \subseteq A$ is a multiplicatively closed subset, then $S^{-1}\,\mathrm{P}^k_{C/A} \simeq \mathrm{P}^k_{S^{-1}C/S^{-1}A}$.

Furthermore, under some finiteness conditions, we obtain also a good localization property for the modules of differential operators.

Corollary 3.35. *Let C be an A-algebra of finite presentation and let M be any C-module. For every multiplicatively closed subset $S \subseteq A$, there is a natural isomorphism*

$$S^{-1}\,\mathrm{Diff}^k_A(C, M) \simeq \mathrm{Diff}^k_{S^{-1}A}(S^{-1}C, S^{-1}M).$$

Proof. By Proposition 3.32, we have $S^{-1}\,\mathrm{Diff}^k_A(C, M) \simeq S^{-1}\,\mathrm{Hom}_A(\mathrm{P}^k_{C/A}, M)$. Then, by Proposition 3.33, the C-module $\mathrm{P}^k_{C/A}$ has finite presentation. Since localization is flat, we can apply Lemma 1.24 to obtain an isomorphism $S^{-1}\,\mathrm{Hom}_A(\mathrm{P}^k_{C/A}, M) \to \mathrm{Hom}_{S^{-1}A}(\mathrm{P}^k_{S^{-1}C/S^{-1}A}, S^{-1}M)$. Finally, by Proposition 3.32, we have

$$\mathrm{Hom}_{S^{-1}A}(\mathrm{P}^k_{S^{-1}C/S^{-1}A}, S^{-1}M) \simeq \mathrm{Diff}^k_{S^{-1}A}(S^{-1}C, S^{-1}M)$$

and this completes the proof. □

3.2.2. Extension of differential operators along Galois extensions

For this subsection, we restrict ourselves to the setting of prime characteristic p rings. The aim of this subsection is to establish a technical result on extension of differential operators (Proposition 3.39). More precisely, given a ring extension $A \subseteq C$ of finite exponent such that $A[C^p] \subseteq C$ is Galois, we prove that every A-differential operator on $A[C^p]$ of order at most k can be extended (locally) to an A-differential operator of C of order at most pk.

We begin with some basic properties of the bracket and the differential operators in prime characteristic.

Lemma 3.36. *Let C be an A-algebra and let M be a C-module. For any A-linear map $D\colon C \to M$ and $x \in C$, we have*

$$[\underbrace{x,[\cdots,[x}_{p},D]\cdots]] = [x^p, D].$$

Proof. We first give an alternative expression for the bracket. Recall that $\mathrm{Hom}_A(C,M)$ has both natural structures of left C-module and right C-module, where left and right multiplication by $x \in C$ are given respectively by

$$L_x, R_x\colon \mathrm{Hom}_A(C,M) \to \mathrm{Hom}_A(C,M) \quad L_x(D) = x \circ D \quad \text{and} \quad R_x(D) = D \circ x.$$

Then it is clear that the bracket defined in 3.26 can be expressed also as $[x, D] = (L_x - R_x)(D)$. Since L_x and R_x commute, we have

$$[\underbrace{x,[\cdots,[x}_{p},D]\cdots]] = (L_x - R_x)^p(D) = (L_x^p - R_x^p)(D) = [x^p, D].$$

□

The following proposition shows that the filtration of the homomorphism module in terms of the modules of differential operators, established in observation (2) from the discussion 3.30, is exhaustive for finite ring extensions of finite exponent.

Proposition 3.37. *Let $A \subseteq C$ be a finite ring extension of finite exponent and let M be a C-module. Then there exists $k \geq 0$ such that* $\mathrm{Diff}_A^k(C,M) = \mathrm{Diff}_A(C,M) = \mathrm{Hom}_A(C,M)$.

Proof. Let $e := \exp(C/A)$ and let S be a finite generating set for C as an A-algebra, say $|S| = r$. We set $k := rp^e - 1$. We claim that any A-linear map $D\colon C \to M$ is a differential operator of order at most k. By the reduction to generators property (see Lemma 3.27.(4)), this holds if we show that $[s_0, [s_1, [\ldots, [s_k, D]\ldots]]] = 0$ for any $s_0, \ldots, s_k \in S$ from the generating set. Since S contains exactly r elements, among any $k+1 = rp^e$ collection of elements $s_0, \ldots, s_k \in S$, there must be one which appears at least p^e times. By the symmetry of the bracket (see Lemma 3.27.(2)), we may assume

that the last p^e elements in $s_0, \dots, s_k$ are all equal to a single element, say s. So we have

$$[s_0, [s_1, [\dots, [s_k, D]\dots]]] = [s_0, [s_1, [\dots, [s_{k-p^e}, [\underbrace{s, [\dots, [s}_{p^e}, D]]]]\dots]]]$$

Now we apply e times the formula for the composition from Lemma 3.36 to the above expression, so we obtain

$$[s_0, [s_1, [\dots, [s_{k-p^e}, [\underbrace{s, [\dots, [s}_{p^e}, D]]]]\dots]]] = [s_0, [s_1, [\dots, [s_{k-p^e}, [s^{p^e}, D]]\dots]]].$$

Note that the last expression is zero because $s^{p^e} \in A$ and D is an A-linear map. This completes the proof. □

We study first the restriction of differential operators of an A-algebra C to the A-subalgebra $C^{[1]} := A[C^p]$.

Proposition 3.38. *Let C be an A-algebra. Let M be a C-module. Then the restriction map*

$$\mathrm{res}\colon \mathrm{Hom}_A(C, M) \to \mathrm{Hom}_A(C^{[1]}, M), \quad D \mapsto D|_{C^{[1]}},$$

is a morphism of left C-modules, and for any $k \geq 0$, it induces a restriction map

$$\mathrm{res}\colon \mathrm{Diff}_A^{pk}(C, M) \to \mathrm{Diff}_A^k(C^{[1]}, M).$$

Equivalently, if $D\colon C \to M$ is an A-differential operator of order at most pk, then its restriction $D\colon C^{[1]} \to M$ is an A-differential operator of order at most k.

Proof. It is clear that $\mathrm{res}\colon \mathrm{Hom}_A(C, M) \to \mathrm{Hom}_A(C^{[1]}, M)$ is an homomorphism of left C-modules. We prove that there is a restriction map $\mathrm{Diff}_A^{pk}(C, M) \to \mathrm{Diff}_A^k(C^{[1]}, M)$ induced by the former restriction. Let $D \in \mathrm{Diff}_A^{pk}(C, M)$ and denote by $\partial := D|_{C^{[1]}}$ the restriction of D to $C^{[1]}$. We prove that ∂ is a differential operator of order at most k, so we have to check that $[x_0[x_1[\dots, [x_k, D]\dots]]] = 0$ for all $x_0, \dots, x_k \in C$. Recall that $C^p = \{c^p : c \in C\}$ is a set of generators for $C^{[1]}$ as A-algebra, by definition. Hence, using the reduction to generators property (see Lemma 3.27.(4)), we have that $\partial \in \mathrm{Diff}_A^k(C^{[1]}, M)$ if

$$[s_0^p, [s_1^p, [\dots, [s_k^p, \partial]\dots]]] = 0 \in \mathrm{Hom}_A(C^{[1]}, M) \quad \text{for all } s_0, \dots, s_k \in C.$$

Note that this holds if, in particular, $[s_0^p, [s_1^p, [\dots, [s_k^p, D]\dots]]] = 0$ in $\mathrm{Hom}_A(C, M)$. Using the formula for the composition from Lemma 3.36, we can express

$$[s_0^p, [s_1^p, [\dots, [s_k^p, D]\dots]]] = [\underbrace{s_0, [\dots, [s_0}_{p}, [\underbrace{s_1, [\dots, [s_1}_{p}, [\dots, [\underbrace{s_k, [\dots, [s_k}_{p}, D]\dots]]\dots]]\dots]]\dots]]\dots]].$$

Note that there are $pk + p$ terms inside the bracket. Then, since D is a differential operator of order at most pk, we conclude that the above expression is zero. □

We study now the extension of differential operators of the A-subalgebra $C^{[1]}$ to differential operators in C. The next proposition shows that if C has a p-basis over $C^{[1]}$, then any A-differential operator $D\colon C^{[1]} \to M$ can be extended to an A-differential operator from C to M. In particular, this result implies that the restriction map $\mathrm{Diff}_A^{pk}(C,M) \to \mathrm{Diff}_A^k(C^{[1]},M)$, defined above in Proposition 3.38, is surjective. We warn the reader that a similar formulation of the next result was proved under much stronger assumptions in [56, Lemma 3.3] with completely different techniques.

Proposition 3.39. *Let $A \subseteq C$ be a ring extension of finite exponent. Assume that $C^{[1]} \subseteq C$ admits a p-basis $\{x_1,\dots,x_n\}$. Let M be a C-module. For each A-linear map $\partial\colon C^{[1]} \to M$, we define an A-linear map $D\colon C \to M$ by the formula*

$$D\left(\sum c_\alpha \mathbf{x}^\alpha\right) = \sum \mathbf{x}^\alpha \partial(c_\alpha),$$

where $c_\alpha \in C^{[1]}$ and the sum is taken over the reduced monomials $\mathbf{x}^\alpha := x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n}$, with $0 \le \alpha_i < p$. Then there is an extension map

$$\mathrm{ext}\colon \mathrm{Hom}_A(C^{[1]},M) \to \mathrm{Hom}_A(C,M), \quad \partial \mapsto D$$

that is a morphism of left C-modules such that $\mathrm{res}\circ\mathrm{ext} = \mathrm{Id}$, and for each $k \ge 0$, this map induces an extension map

$$\mathrm{ext}\colon \mathrm{Diff}_A^k(C^{[1]},M) \to \mathrm{Diff}_A^{pk}(C,M).$$

Equivalently, if $\partial\colon C^{[1]} \to M$ is an A-differential operator of order at most k, then $D\colon C \to M$ is an A-differential operator of order at most pk.

Proof. It is clear that $\mathrm{ext}\colon \mathrm{Hom}_A(C^{[1]},M) \to \mathrm{Hom}_A(C,M)$ is an homomorphism of left C-modules such that $\mathrm{res}\circ\mathrm{ext}$ is the identity. We now prove by induction on the order k that if $\partial\colon C^{[1]} \to M$ is an A-differential operator of order at most k, then $D\colon C \to M$ is an A-differential operator of order at most pk.

Let $k = 0$. Recall from (1) in discussion 3.30 that there are natural identifications of $C^{[1]}$-modules $\mathrm{Diff}_A^0(C^{[1]},M) \simeq \mathrm{Hom}_{C^{[1]}}(C^{[1]},M) \simeq M$. Then any A-differential operator $\partial\colon C^{[1]} \to M$ of order zero is a $C^{[1]}$-linear map and can be identified with the multiplication by some fixed element $m \in M$. That is, there is $m \in M$ such that $\partial(c) = cm$ for all $c \in C^{[1]}$. Hence, it follows from the definition of D that $D(c) = cm$ for all $c \in C$. Therefore, since $\mathrm{Diff}_A^0(C,M) \simeq \mathrm{Hom}_C(C,M) \simeq M$ as C-modules (see (1) in discussion 3.30), we conclude that D is an A-differential operator of order $0 = p\cdot 0$, and the assertion is true.

Assume that $k > 0$. For each A-differential operator $\partial\colon C^{[1]} \to M$ of order at most k, we have to show that the map $D\colon C \to M$ defined in the statement is an A-differential operator of order at most pk. That is, we have to show that $[f_0,[f_1,[\ldots[f_{pk},D]\ldots]]] = 0$ for all $f_0,\dots,f_{pk} \in C$. Recall that $C = C^{[1]}[x_1,\dots,x_n]$, since $x_1,\dots,x_n$ is a p-basis for C over $C^{[1]}$. In addition, since $C^{[1]} = A[C^p]$ and $A \subset C$ has finite exponent, we have that $x_1,\dots,x_n$ generate C as an A-algebra. That is, $C = A[x_1,\dots,x_n]$ and any element in C is an A-linear combination of monomials

$\mathbf{x}^\beta := x_1^{\beta_1} \cdot \ldots \cdot x_n^{\beta_n}$ with $\beta_i \in \mathbb{N}_0$. Therefore, by the reduction to generators property (see Lemma 3.27.(4)), it is enough to show that

$$[x_{i_0}, [x_{i_1}, [\ldots [x_{i_{pk}}, D] \ldots]]]] = 0 \quad \forall x_{i_0}, \ldots, x_{i_{pk}} \in \{x_1, \ldots, x_n\}. \tag{3.39.1}$$

With this aim, we first state a property on the evaluation of D at some monomials that will be used successively in the proof. Observe that any monomial $\mathbf{x}^\beta \in C$, not necessarily reduced, admits a unique reduced expression $\mathbf{x}^\beta = c\mathbf{x}^{\beta'}$, where $c \in C^{[1]}$ and $\mathbf{x}^{\beta'}$ is a reduced monomial. In fact, for a monomial $\mathbf{x}^\beta := x_1^{\beta_1} \cdot \ldots \cdot x_n^{\beta_n} \in C$, there is a unique expression $\beta_i = q_i p + r_i$ with $0 \leq r_i < p$, and we can write $\mathbf{x}^\beta = c\mathbf{x}^{\beta'}$ where

$$c = (x_1^{q_1})^p \cdot \ldots \cdot (x_n^{q_n})^p \in C^{[1]} \quad \text{and} \quad \mathbf{x}^{\beta'} = x_1^{r_1} \cdot \ldots \cdot x_n^{r_n}.$$

Then for any monomial $\mathbf{x}^\beta \in C$ with reduced form $\mathbf{x}^\beta = c\mathbf{x}^{\beta'}$, we have $D(\mathbf{x}^\beta) = \partial(c)\mathbf{x}^{\beta'}$. In particular, for $\mathbf{x}^\beta := x_{l+1}^{\beta_{l+1}} \cdot \ldots \cdot x_n^{\beta_n}$ and $\mathbf{x}^\alpha := x_1^{\alpha_1} \cdot \ldots \cdot x_l^{\alpha_l}$ reduced, the product $\mathbf{x}^\alpha \cdot \mathbf{x}^\beta$ is again a monomial whose reduced form is $\mathbf{x}^\alpha\mathbf{x}^\beta = c\mathbf{x}^\alpha\mathbf{x}^{\beta'}$ and we have

$$D(\mathbf{x}^\alpha\mathbf{x}^\beta) = \partial(c)\mathbf{x}^\alpha\mathbf{x}^{\beta'} = \mathbf{x}^\alpha D(\mathbf{x}^\beta)\ . \tag{*}$$

We now prove (3.39.1). We divide the proof in two cases according to the number of times that each element x_j of the p-basis appears in the list $x_{i_0}, \ldots, x_{i_{pk}}$ from the bracket $[x_{i_0}, [x_{i_1}, [\ldots [x_{i_{pk}}, D] \ldots]]]$.

Case I: There is $j \in \{1, \ldots, n\}$ such that x_j appears at least p times in the list $x_{i_0}, \ldots, x_{i_{pk}}$. Using the symmetry of the bracket (see Lemma 3.27.(2)), we may assume that the last p terms in the list $x_{i_0}, \ldots, x_{i_{pk}}$ are all equal to x_j. Then, by the formula from Lemma 3.36, we have

$$[x_{i_0}, [x_{i_1}, [\ldots [x_{i_{pk}}, D] \ldots]]] = [x_{i_0}, [x_{i_1}, [\ldots [x_{i_{p(k-1)}}, [x_j^p, D]] \ldots]]]\ . \tag{3.39.2}$$

Note that the map $[x_j^p, D]\colon C \to M$ can be obtained from $[x_j^p, \partial]\colon C^{[1]} \to M$ in a similar way to how the map D is defined from ∂. More precisely,

$$[x_j^p, D]\left(\sum c_\alpha \mathbf{x}^\alpha\right) = \sum \left(x_j^p \partial(c_\alpha)\mathbf{x}^\alpha - \partial(c_\alpha x_j^p)\mathbf{x}^\alpha\right) = \sum [x_j^p, \partial](c_\alpha) \cdot \mathbf{x}^\alpha.$$

By (3) in discussion 3.30, we know that $[x_j^p, \partial]$ is an A-differential operator from $C^{[1]}$ to M of order at most $k-1$. Then, by the inductive hypothesis, $[x_j^p, D]$ is an A-differential operator from C to M of order at most $p(k-1)$. Therefore, the right term in (3.39.2) is zero and the proof for this case is complete.

Case II: Every x_j appears at most $p-1$ times in the list $x_{i_0}, \ldots, x_{i_{pk}}$. Reordering $x_1, \ldots, x_n$ if necessary, we may assume that only the first m elements $x_1, \ldots, x_m$ of the p-basis appear on the list. We denote by r_i the number of times that each x_i appears on the list. Note that $1 \leq r_i < p$ and $r_1 + \cdots + r_m = pk + 1$. Then, using the symmetry of the bracket (see Lemma 3.27.(2)), we can rearrange the terms inside of the brackets as

$$[x_{i_0}, [x_{i_1}, [\ldots [x_{i_{pk}}, D] \ldots]]] = \tag{3.39.3}$$
$$[\underbrace{x_1, [\ldots, [x_1}_{r_1}, \underbrace{[x_2, [\ldots, [x_2}_{r_2}, [\ldots, \underbrace{[x_m, [\ldots, [x_m}_{r_m}, D] \ldots]] \ldots]] \ldots]] \ldots]] \ldots]].$$

Since $[x_{i_0}, [x_{i_1}, [\dots [x_{i_{pk}}, D]\dots]]]$ is an A-linear operator from C to M and $x_1, \dots, x_n$ is a p-basis for C over $C^{[1]}$, it is enough to show that its evaluation at $c\mathbf{x}^\alpha$, for any $c \in C^{[1]}$ and $\mathbf{x}^\alpha \in C$ reduced monomial, is zero.

Let $c\mathbf{x}^\alpha \in C$ where $c \in C^{[1]}$ and $\mathbf{x}^\alpha$ is a reduced monomial. For any integer $r > 0$, set $[r] := \{1, \dots, r\}$. Then, by Lemma 3.29, the expression in (3.39.3) evaluated at $c\mathbf{x}^\alpha$ is

$$\begin{aligned}
&[\underbrace{x_1, [\dots, [x_1}_{r_1}, [\underbrace{x_2, [\dots, [x_2}_{r_2}, [\dots, [\underbrace{x_m, [\dots, [x_m}_{r_m}, D]\dots]]\dots]]\dots]]\dots]](c\mathbf{x}^\alpha) \\
&= \sum_{\substack{S_i \subseteq [r_i] \\ i=1,\dots,m}} \prod_{i=1}^{m} \left((-1)^{r_i - |S_i|} x_i^{|S_i|} \cdot D \right) \left(c\mathbf{x}^\alpha \cdot \prod_{i=1}^{m} x_i^{r_i - |S_i|} \right) \left(\right. \qquad (3.39.4) \\
&= \sum_{\substack{S_i \subseteq [r_i] \\ i=1,\dots,m}} \prod_{i=1}^{m} \left((-1)^{r_i - |S_i|} x_i^{|S_i|} \cdot D \right) \left(c x_{m+1}^{\alpha_{m+1}} \cdots x_n^{\alpha_n} \cdot \prod_{i=1}^{m} x_i^{r_i + \alpha_i - |S_i|} \right) \left(. \right.
\end{aligned}$$

Using the property (*) stated at the beginning of the proof, we have

$$D \left(c x_{m+1}^{\alpha_{m+1}} \cdots x_n^{\alpha_n} \cdot \prod_{i=1}^{m} x_i^{r_i + \alpha_i - |S_i|} \right) = x_{m+1}^{\alpha_{m+1}} \cdots x_n^{\alpha_n} \cdot D \left(c \prod_{i=1}^{m} x_i^{r_i + \alpha_i - |S_i|} \right) \left(\right.$$

So the term $x_{m+1}^{\alpha_{m+1}} \cdots x_n^{\alpha_n}$ can be factored out from the last expression in (3.39.4). Thus, the evaluation at $c\mathbf{x}^\beta$ of (3.39.3) is zero, that is,

$$[x_{i_0}, [x_{i_1}, [\dots [x_{i_{pk}}, D]\dots]]](c\mathbf{x}^\alpha) = 0$$

if the following expression is also zero:

$$\sum_{\substack{S_i \subseteq [r_i] \\ i=1,\dots,m}} \prod_{i=1}^{m} \left((-1)^{r_i - |S_i|} x_i^{|S_i|} \cdot D \right) \left(c \cdot \prod_{i=1}^{m} x_i^{r_i + \alpha_i - |S_i|} \right) \left(. \right. \qquad (3.39.5)$$

To prove that the expression (3.39.5) above is zero, we consider two subcases depending on the values $r_i + \alpha_i$ for $i = 1, \dots, m$.

Case II.1: There is an index $i \in \{1, \dots, m\}$ such that $r_i + \alpha_i < p$. Reordering $x_1, \dots, x_m$ if necessary, we may assume that $i = 1$. Note that $r_1 + \alpha_1 - |S_1| < p$ by hypothesis, so the monomial $x_1^{r_1 + \alpha_1 - |S_1|}$ is reduced. Then, we can apply property (*) to each term of the expression (3.39.5), and obtain

$$D \left(c \cdot \prod_{i=1}^{m} x_i^{r_i + \alpha_i - |S_i|} \right) = x_1^{r_1 + \alpha_1 - |S_1|} \cdot D \left(c \cdot \prod_{i=2}^{m} x_i^{r_i + \alpha_i - |S_i|} \right) \left(\right.$$

Hence, the expression in (3.39.5) becomes

$$\sum_{\substack{S_i\subseteq[r_i]\\ i=1,\dots,m}} (-1)^{r_1-|S_1|}x_1^{r_1+\alpha_1}\prod_{i=2}^{m}\Big((-1)^{r_i-|S_i|}x_i^{|S_i|}\cdot D\quad c\cdot\prod_{i=1}^{m}x_i^{r_i+\alpha_i-|S_i|}\Big)\Big($$

$$=\Bigg(\sum_{S_1\subseteq[r_1]}\Big((-1)^{r_1-|S_1|}\Big)\Big(x_1^{r_1+\alpha_1}\sum_{\substack{S_i\subseteq[r_i]\\ i=2,\dots,m}}\prod_{i=2}^{m}(-1)^{r_i-|S_i|}x_i^{|S_i|}\cdot D\quad c\cdot\prod_{i=1}^{m}x_i^{r_i+\alpha_i-|S_i|}\Big)\Big($$

This expression is zero, because the first term in the product is

$$\sum_{S_1\subseteq[r_1]}(-1)^{r_1-|S_1|}=\sum_{l=0}^{r_1}\Big((-1)^{r_1-l}\binom{r_1}{l}=(1-1)^{r_1}=0.$$

This completes the proof for the first of the two subcases. We prove the one that lefts.

Case II.2: For every $i\in\{1,\dots,m\}$, we have $r_i+\alpha_i\geq p$. For a collection $S=(S_1,\dots,S_m)$ of subsets $S_i\subseteq[r_i]$, we define $U_S:=\{1\leq i\leq m : r_i+\alpha_i-|S_i|\geq p\}$. Then the expression in (3.39.5) can be written as

$$\sum_{\substack{S=(S_1,\dots,S_m)\\ S_i\subseteq[r_i]}}\prod_{i=1}^{m}\Big((-1)^{r_i-|S_i|}x_i^{|S_i|}\cdot D\left(c\cdot\prod_{i\in U_S}x_i^{r_i+\alpha_i-|S_i|}\prod_{i\notin U_S}x_i^{r_i+\alpha_i-|S_i|}\right)\Big(\tag{3.39.6}$$

Note that $x_i^{r_i+\alpha_i-|S_i|}$ is a reduced monomial for all $i\notin U_S$. Hence, using property (*), we have

$$D\left(\Big(c\cdot\prod_{i\in U_S}x_i^{r_i+\alpha_i-|S_i|}\prod_{i\notin U_S}x_i^{r_i+\alpha_i-|S_i|}\right)=\prod_{i\notin U_S}\Big(x_i^{r_i+\alpha_i-|S_i|}\cdot D\left(c\cdot\prod_{i\in U_S}\Big(x_i^{r_i+\alpha_i-|S_i|}\right)\Big($$

So we can rewrite the expression in (3.39.6) as:

$$\sum_{\substack{S=(S_1,\dots,S_m)\\ S_i\subseteq[r_i]}}\prod_{i=1}^{m}(-1)^{r_i-|S_i|}x_i^{|S_i|}\prod_{i\notin U_S}\Big(x_i^{r_i+\alpha_i-|S_i|}\cdot D\left(c\cdot\prod_{i\in U_S}x_i^{r_i+\alpha_i-|S_i|}\right)\Big(\tag{3.39.7}$$

Observe that if $i\in U_S$, then $r_i+\alpha_i-|S_i|=p+l_i$ for some $l_i<p$, since $r_i,\alpha_i<p$. Thus, we can write

$$c\cdot\prod_{i\in U_S}\Big(x_i^{r_i+\alpha_i-|S_i|}=c\cdot\prod_{i\in U_S}x_i^{p}\prod_{i\in U_S}\Big(x_i^{l_i},$$

where $c\cdot\prod_{i\in U_S}x_i^p\in C^{[1]}$ and $\prod_{i\in U_S}x_i^{l_i}$ is a reduced monomial. Using this factorization in (3.39.7) and applying the definition of D, we obtain the following equivalent expression:

$$\sum_{\substack{S=(S_1,\dots,S_m)\\ S_i\subseteq[r_i]}}\prod_{i=1}^{m}\Big((-1)^{r_i-|S_i|}x_i^{|S_i|}\prod_{i\notin U_S}x_i^{r_i+\alpha_i-|S_i|}\prod_{i\in U_S}x_i^{l_i}\cdot\partial\left(c\cdot\prod_{i\in U_S}x_i^{p}\right)\Big(\Big($$

Recall that $l_i = r_i + \alpha_i - |S_i| - p$ for $i \in U_S$, so by regrouping some terms, the above expression becomes

$$\sum_{\substack{S=(S_1,\dots,S_m)\\ S_i\subseteq[r_i]}} \prod_{i=1}^{m}(-1)^{r_i-|S_i|} \prod_{i\notin U_S} x_i^{r_i+\alpha_i} \prod_{i\in U_S} x_i^{r_i+\alpha_i-p} \cdot \partial\left(c\left(\prod_{i\in U_S}\left(x_i^p\right)\right.\right.$$

$$= \sum_{\substack{S=(S_1,\dots,S_m)\\ S_i\subseteq[r_i]}} \prod_{i=1}^{m}(-1)^{r_i-|S_i|} x_i^{r_i+\alpha_i-p} \prod_{i\notin U_S} x_i^{p} \cdot \partial\left(c\left(\prod_{i\in U_S}\left(x_i^p\right)\right.\right.\left(\right.$$

$$= \prod_{i=1}^{m} x_i^{r_i+\alpha_i-p}\left)\left(\sum_{\substack{S=(S_1,\dots,S_m)\\ S_i\subseteq[r_i]}} \prod_{i=1}^{m}(-1)^{r_i-|S_i|} \prod_{i\notin U_S} x_i^{p} \cdot \partial\left(c\left(\prod_{i\in U_S}\left(x_i^p\right)\right.\right.\right.\left(\right.$$

By rearranging the above sum over $S = (S_1, \dots, S_m)$ according to the resulting subsets $U_S \subseteq [m]$, the expression becomes

$$\prod_{i=1}^{m} x_i^{r_i+\alpha_i-p}\left)\left(\sum_{U\subseteq[m]} \sum_{\substack{S=(S_1,\dots,S_m)\\ S_i\subseteq[r_i],\ U_S=U}} \prod_{i=1}^{m}(-1)^{r_i-|S_i|} \prod_{i\notin U}\left(x_i^p \cdot \partial \quad c\cdot\prod_{i\in U} x_i^p\right)\right.\right.$$

$$= \prod_{i=1}^{m}\left(x_i^{r_i+\alpha_i-p}\right) \cdot \sum_{U\subseteq[m]}\left(\sigma_U \cdot \prod_{i\notin U} x_i^p \cdot \partial \quad c\cdot\prod_{i\in U} x_i^p\right)\left(\right. \tag{3.39.8}$$

where

$$\sigma_U := \sum_{\substack{S=(S_1,\dots,S_m)\\ S_i\subseteq[r_i],\ U_S=U}} \prod_{i=1}^{m}(-1)^{r_i-|S_i|}$$

$$= \prod_{i\in U}\left(\left(\sum_{\substack{S_i\subseteq[r_i],\\ r_i+\alpha_i-|S_i|\geq p}}(-1)^{r_i-|S_i|}\right)\right.\left.\left.\prod_{i\notin U}\left(\left(\sum_{\substack{S_i\subseteq[r_i],\\ r_i+\alpha_i-|S_i|<p}}(-1)^{r_i-|S_i|}\right)\right)\right.\right.\left(\right.$$

Note that the last equality in the expression for σ_U follows since finite sums can be exchanged with finite products and the subsets $S_1, \dots, S_m$ are independent of each other in the expression of σ_U.

We now claim that $\sigma_U = (-1)^{|U|} \cdot \mu$, for some integer μ independent from the subset $U \subseteq [m]$. Suppose that $U \subset [m]$ is a proper subset and let $V = U \cup \{j\} \subseteq [m]$ for some $j \notin U$. Observe that σ_U and σ_V have the same factors except the one corresponding to j. Indeed,

$$\sigma_U = \left(\left(\sum_{\substack{S_j\subset[r_j],\\ r_j+\alpha_j-|S_j|<p}}(-1)^{r_j-|S_j|}\right)\right.\left.\left.\prod_{i\in U}\left(\left(\sum_{\substack{S_i\subset[r_i],\\ r_i+\alpha_i-|S_i|\geq p}}(-1)^{r_i-|S_i|}\right)\right)\right.\right.\left.\left.\prod_{\substack{i\notin U\\ i\neq j}}\left(\left(\sum_{\substack{S_i\subset[r_i],\\ r_i+\alpha_i-|S_i|<p}}(-1)^{r_i-|S_i|}\right)\right)\right.\right.\left(\right.,$$

$$\sigma_V = \left(\sum_{\substack{S_j\subset[r_j],\\ r_j+\alpha_j-|S_j|\geq p}} (-1)^{r_j-|S_j|}\right)\left(\prod_{i\in U}\left(\sum_{\substack{S_i\subset[r_i],\\ r_i+\alpha_i-|S_i|\geq p}} (-1)^{r_i-|S_i|}\right)\right)\left(\prod_{\substack{i\notin U\\ i\neq j}}\left(\sum_{\substack{S_i\subset[r_i],\\ r_i+\alpha_i-|S_i|<p}} (-1)^{r_i-|S_i|}\right)\right),$$

and the last two products on both expressions coincide. Therefore, we have that $\sigma_U + \sigma_V = 0$, because

$$\sum_{\substack{S_j\subseteq[r_j],\\ r_j+\alpha_j-|S_j|<p}} (-1)^{r_j-|S_j|} + \sum_{\substack{S_j\subseteq[r_j],\\ r_j+\alpha_j-|S_j|\geq p}} (-1)^{r_j-|S_j|} = \sum_{S_j\subseteq[r_j]} (-1)^{r_j-|S_j|}$$

$$= \sum_{l=0}^{r_j} (-1)^{r_j-l}\binom{r_j}{l} = (1-1)^{r_j} = 0.$$

This implies that $\sigma_V = -\sigma_U$. Let $\mu = \sigma_\emptyset$, then by induction on $|U|$ it is clear that $\sigma_U = (-1)^{|U|}\cdot\mu$ for all $U\subseteq[m]$.

Hence, we can simplify the expression in (3.39.8) to

$$\left(\prod_{i=1}^{m} x_i^{r_i+\alpha_i-p}\right)\left(\sum_{U\subseteq[m]}\left((-1)^{|U|}\cdot\mu\cdot\prod_{i\notin U} x_i^p\cdot\partial \quad \prod_{i\in U} x_i^p c\right)\right.\!.$$

Finally, using the formula from Lemma 3.28, we observe that the above expression coincides with

$$\mu\cdot \left(\prod_{i=1}^{m} x_i^{r_i+\alpha_i-p}\right)\left(x_1^p,[\ldots,[x_m^p,\partial]\ldots]](c), \tag{3.39.9}$$

which is our final expression for (3.39.5). To conclude recall that $pk+1 = r_1+\cdots+r_m < pm$, so that $m\geq k+1$. Since $\partial\colon C^{[1]}\to M$ is an A-differential operator of order at most k, the above term in (3.39.9) is zero. This completes the proof of the second subcase, so we have covered all the cases. □

Corollary 3.40. *Let $A\subseteq C$ be a finite ring extension of finite exponent. If C has a p-basis over $C^{[1]}$, then for each $k\geq 0$ the restriction map* res: $\mathrm{Diff}^{pk}_A(C,M)\to \mathrm{Diff}^k_A(C^{[1]},M)$ *is surjective for any C-module M.*

3.2.3. Purely inseparable extensions, differential operators and modules of principal parts

We continue in the setting of rings with prime characteristic p. We use the previous result on extension of differential operators (Proposition 3.39) to give a new characterization of purely inseparable extensions in terms of the modules of differential operators (Theorem 3.48). Moreover, we re-obtain the characterization in terms of the modules of principal parts for purely inseparable extensions given by P. Sancho de Salas in [56, Theorem 3.8].

We study first the modules of differential operators and the modules of principal parts of a purely inseparable extension. In particular, we begin with a certain subclass

of purely inseparable extensions, namely, modular extensions with splitting p-basis. These class of extensions will be studied later with more detail in Chapter 4 from this thesis.

Proposition 3.41. *Let A be a ring and let $C = A[x_1, \ldots, x_n]$ be an A-algebra with defining relations $x_1^{p^{e_1}} = \cdots = x_n^{p^{e_n}} = 0$ for some integers $e_i > 0$. Set $\mathcal{A} := \{\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n : 0 \leq \alpha_j < p^{e_j}\}$. Then*

(1) $\mathrm{P}^k_{C/A}$ is a finite free C-module for all $k \geq 0$.

(2) For each $\alpha \in \mathcal{A}$, the A-linear map $\Delta_\alpha \colon C \to C$ defined as

$$\Delta_\alpha(\mathbf{x}^\beta) = \binom{\beta}{\alpha}\mathbf{x}^{\beta-\alpha}$$

is a differential operator of order $|\alpha| := \alpha_1 + \ldots + \alpha_n$.

(3) Let M be a C-module. Then each differential operator $D \colon C \to M$ of order at most k can be written uniquely as

$$D = \sum_{\substack{\alpha \in \mathcal{A} \\ |\alpha| \leq k}} m_\alpha \cdot \Delta_\alpha, \quad m_\alpha \in M.$$

Proof. We first prove (1). Note that, under these hypothesis, C is a free A-module with basis formed by the monomials $\{\mathbf{x}^\alpha : \alpha \in \mathcal{A}\}$. Since the presentation of an algebra is preserved by base change, the (left) C-algebra $C \otimes_A C$ obtained from C by application of the base change $A \to C$ has presentation $C \otimes_A C = C[1 \otimes x_1, \ldots, 1 \otimes x_n]$ with defining relations $(1 \otimes x_i)^{p^{e_i}} = 0$ for $i = 1, \ldots, n$. We can make a change of generators, so $C \otimes_A C = C[z_1, \ldots, z_n]$ where $z_i := 1 \otimes x_i - x_i \otimes 1$ and the defining relations are $z_i^{p^{e_i}} = 0$ for $i = 1, \ldots, n$. Then it is clear that $C \otimes_A C$ is a free C-module with basis given by the monomials $\{\mathbf{z}^\alpha : \alpha \in \mathcal{A}\}$.

Let J be the kernel of the multiplication map $C \otimes_A C \to C$ as in discussion 3.31. Note that J is generated as an ideal by $z_1, \ldots, z_n$. Hence, for each $k \geq 0$, the ideal J^{k+1} is a free C-module generated by the subset of monomials $\{\mathbf{z}^\alpha : \alpha \in \mathcal{A}, |\alpha| \geq k+1\}$. Since $\mathrm{P}^k_{C/A} = (C \otimes_A C)/J^{k+1}$, we conclude that $\mathrm{P}^k_{C/A}$ is a free C-module generated by the classes of the monomials in $\{\mathbf{z}^\alpha : \alpha \in \mathcal{A}, |\alpha| \leq k\}$.

Now we show that the A-linear maps Δ_α in (2) are differential operators. Let $\{\varphi_\alpha \colon C \otimes_A C \to C : \alpha \in \mathcal{A}\}$ be the dual basis for $\mathrm{Hom}_C(C \otimes_A C, C)$ of the basis $\{\mathbf{z}^\alpha : \alpha \in \mathcal{A}\}$ for $C \otimes_A C$. Recall that there is a natural identification $\mathrm{Hom}_C(C \otimes_A C, C) = \mathrm{End}_A(C)$, as we noted in 1.22. Let $\Delta_\alpha \colon C \to C$ be the A-endomorphisms of C corresponding to $\varphi_\alpha \colon C \otimes_A C \to C$ via this identification. Then, for any $\beta \in \mathcal{A}$, we have

$$\Delta_\alpha(\mathbf{x}^\beta) = \varphi_\alpha(1 \otimes \mathbf{x}^\beta) = \varphi_\alpha((\mathbf{z} + \mathbf{x} \otimes 1)^\beta) = \varphi_\alpha\left(\left(\sum_{\substack{\gamma \in \mathcal{A} \\ |\gamma| \leq |\beta|}} \binom{\beta}{\gamma}\mathbf{x}^{\beta-\gamma}\mathbf{z}^\gamma\right)\right) = \binom{\beta}{\alpha}\mathbf{x}^{\beta-\alpha}.$$

Note also that Δ_α is differential operator of order at most k if and only if φ_α is zero on J^{k+1}. This occurs if and only if $|\alpha| \leq k$. Hence, Δ_α is a differential operator of order $|\alpha|$ and this completes the proof of (2).

We finally prove (3). Let M be a C-module. Since $\{\varphi_\alpha : \alpha \in \mathcal{A}\}$ is a basis for $\mathrm{Hom}_C(C \otimes_A C, C)$, it follows that any homomorphism of C-modules $\varphi\colon C \otimes_A C \to M$ can be written uniquely as

$$\varphi = \sum_{\alpha \in \mathcal{A}} m_\alpha \cdot \varphi_\alpha$$

for certain $m_\alpha \in M$ with $\alpha \in \mathcal{A}$. Recall that the maps φ_α form the dual basis of $\{\mathbf{z}^\alpha : \alpha \in \mathcal{A}\}$, so $m_\alpha = \varphi(\mathbf{z}^\alpha)$. Via the natural identification $\mathrm{Hom}_A(C, M) \cong \mathrm{Hom}_C(C \otimes_A C, M)$, we deduce that any $D \in \mathrm{Hom}_A(C, M)$ can be written uniquely as $D = \sum_{\alpha \in \mathcal{A}} m_\alpha \cdot \Delta_\alpha$ for certain $m_\alpha \in M$. To conclude, we observe that D is an A-differential operator of order at most k if and only if the corresponding map $\varphi : C \otimes_A C \to M$ is zero on J^{k+1}, and this occurs if and only if $m_\alpha = \varphi(\mathbf{z}^\alpha) = 0$ for each $\alpha \in \mathcal{A}$ such that $|\alpha| \geq k + 1$. □

Remark 3.42. In the setting of the above proposition, it is clear that the operators $\{\Delta_\alpha : \alpha \in \mathcal{A}, |\alpha| \leq k\}$ form a basis for $\mathrm{Diff}^k_A(C)$ as C-module.

Using the previous proposition and the fact that the modules of principal parts behave well under base change, we obtain the following conclusions on the modules of principal parts and the modules of differential operators for purely inseparable extensions of rings in general.

Proposition 3.43. *Let $A \subseteq C$ be a purely inseparable ring extension. Then*

(1) $\mathrm{P}^k_{C/A}$ *is a finitely generated projective C-module for all $k \geq 0$.*

(2) $\mathrm{Diff}^k_A(C)$ *is a C-module direct summand of* $\mathrm{End}_A(C)$ *for all $k \geq 0$.*

Proof. We show first that $\mathrm{P}^k_{C/A}$ is a finitely generated projective C-module. By Proposition 1.7, this is equivalent to show that it is flat of finite presentation. On the one hand, since $A \subseteq C$ is purely inseparable, C has finite presentation as A-algebra (Remark 3.13). Hence, $\mathrm{P}^k_{C/A}$ is a C-module of finite presentation by Proposition 3.33.(2). On the other hand, to show that $\mathrm{P}^k_{C/A}$ is flat, it is enough to show that the $C_\mathfrak{p}$-module $C_\mathfrak{p} \otimes_C \mathrm{P}^k_{C/A} = \mathrm{P}^k_{C_\mathfrak{p}/A_\mathfrak{p}}$ is flat for each prime ideal $\mathfrak{p} \subset A$ (see Proposition A.13 and Proposition 3.34).

Since $A \subseteq C$ is purely inseparable, there is a faithfully flat extension $A_\mathfrak{p} \to A'$ such that

$$C' := C_\mathfrak{p} \otimes_{A_\mathfrak{p}} A' = A'[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$$

for some integers $e_i > 0$. We have shown in Proposition 3.41 that $\mathrm{P}^k_{C'/A'}$ is a finite free C'-module, in particular, flat. We also know that $\mathrm{P}^k_{C'/A'} = C' \otimes_{C_\mathfrak{p}} \mathrm{P}^k_{C_\mathfrak{p}/A_\mathfrak{p}}$ (Proposition 3.34). Note that the map $C_\mathfrak{p} \to C'$ is faithfully flat, because it is a base change of the

faithfully flat map $A_{\mathfrak{p}} \to A'$ (Proposition A.16). Therefore, $\mathrm{P}^k_{C_{\mathfrak{p}}/A_{\mathfrak{p}}}$ is a flat $C_{\mathfrak{p}}$-module by faithfully flat descent (Proposition A.15.(2)). This completes the proof of (1).

Now we show that (2) follows easily from (1). Indeed, we consider the exact sequence

$$0 \to J^{k+1} \to C \otimes_A C \to \mathrm{P}^k_{C/A} \to 0,$$

where J is the kernel of the multiplication map $C \otimes_A C \to C$ as in discussion 3.31. We have proved in (1) that $\mathrm{P}^k_{C/A}$ is projective, so the sequence is split exact (Proposition 1.2). Since $\mathrm{Hom}_C(-, C)$ functor preserves split exact sequences, the following exact sequence splits

$$0 \to \mathrm{Hom}_C(J^{k+1}, C) \to \mathrm{Hom}_C(C \otimes_A C, C) \to \mathrm{Hom}_C(\mathrm{P}^k_{C/A}, C) \to 0.$$

Therefore, $\mathrm{Hom}_C(\mathrm{P}^k_{C/A}, C)$ is a C-module direct summand of $\mathrm{Hom}_C(C \otimes_A C, C)$ by Lemma A.10. Using the natural identifications $\mathrm{Hom}_C(\mathrm{P}^k_{C/A}, C) = \mathrm{Diff}^k_A(C)$ and $\mathrm{Hom}_C(C \otimes_A C, C) = \mathrm{End}_A(C)$ (see Proposition 3.32 and discussion 1.22 respectively), we conclude that $\mathrm{Diff}^k_A(C)$ is a C-module direct summand of $\mathrm{End}_A(C)$. □

The purpose of this subsection is to show that the converse to the later proposition holds for certain finite extension of rings $A \subseteq C$ with finite exponent. We first address this tackle from the perspective of the modules of principal parts. To this end we discuss some properties of these modules, in particular, the relation between $\mathrm{P}^{pk}_{C/A}$ and $\mathrm{P}^k_{C^{[1]}/A}$. In what follows, for each integer $e \geq 0$, we denote by

$$\delta^{[e]}_k \colon C^{[e]} \to \mathrm{P}^k_{C^{[e]}/A}$$

the universal differential operator of order k of the A-algebra $C^{[e]}$ (see discussion 3.31).

Lemma 3.44. *Let C be an A-algebra, and let $k \geq 0$. Then there is a unique homomorphism of $C^{[1]}$-modules $\mathrm{P}^k_{C^{[1]}/A} \to \mathrm{P}^{pk}_{C/A}$ such that the following diagram*

$$\begin{array}{ccc} C & \xrightarrow{\delta_{pk}} & \mathrm{P}^{pk}_{C/A} \\ \uparrow & & \uparrow \\ C^{[1]} & \xrightarrow{\delta^{[1]}_k} & \mathrm{P}^k_{C^{[1]}/A} \end{array}$$

commutes.

Proof. Note that $\mathrm{P}^{pk}_{C/A}$ is a $C^{[1]}$-module by restriction of scalars. Recall that δ_{pk} is an A-differential operator of order pk. Then its restriction to $C^{[1]}$ is a differential operator $\mathrm{res}(\delta_{pk}) \colon C^{[1]} \to \mathrm{P}^{pk}_{C/A}$ of order at most k by Proposition 3.38. Thus, by the universal property of $\delta^{[1]}_k$ (see Proposition 3.32), there is a unique homomorphism of $C^{[1]}$-modules $\varphi \colon \mathrm{P}^k_{C^{[1]}/A} \to \mathrm{P}^{pk}_{C/A}$ such that $\varphi \circ \delta^{[1]}_k = \mathrm{res}(\delta_{pk})$. Thus, φ is the desired map that makes the diagram commutative. □

Proposition 3.45. *Let $A \subseteq C$ be a finite ring extension of finite exponent. Then:*

(1) There is a natural homomorphism of C-modules

$$C \otimes_{C^{[1]}} \mathrm{P}^k_{C^{[1]}/A} \to \mathrm{P}^{pk}_{C/A}, \quad 1 \otimes \delta^{[1]}_k c^p \mapsto (\delta_{pk})^p.$$

(2) If C has a p-basis over $C^{[1]}$, then the above map has a retraction

$$\mathrm{P}^{pk}_{C/A} \to C \otimes_{C^{[1]}} \mathrm{P}^k_{C^{[1]}/A}\,.$$

Proof. The homomorphism $C \otimes_{C^{[1]}} \mathrm{P}^k_{C^{[1]}/A} \to \mathrm{P}^{pk}_{C/A}$ from (1) is induced by the homomorphism obtained in Lemma 3.44. To prove (2), we have to show that there is a map $\mathrm{P}^{pk}_{C/A} \to C \otimes_{C^{[1]}} \mathrm{P}^k_{C^{[1]}/A}$ such that the composition with the map in (1) is the identity in $C \otimes_{C^{[1]}} \mathrm{P}^k_{C^{[1]}/A}$. Note that this holds if we show that for any C-module M, the induced map

$$\mathrm{Hom}_C(\mathrm{P}^{pk}_{C/A}, M) \to \mathrm{Hom}_C(C \otimes_{C^{[1]}} \mathrm{P}^k_{C^{[1]}/A}, M) = \mathrm{Hom}_{C^{[1]}}(\mathrm{P}^k_{C^{[1]}/A}, M)$$

is surjective. By the commutativity of the diagram of Lemma 3.44 and the universal properties of δ_{pk} and $\delta^{[1]}_k$ (see Proposition 3.32), this map can be identified with the restriction map

$$\mathrm{res}\colon \mathrm{Diff}^{pk}_A(C, M) \to \mathrm{Diff}^k_A(C^{[1]}, M),$$

from Proposition 3.38, but we have already proved in Corollary 3.40 that this map is surjective under the hypothesis in the statement. □

Using these properties, we show that any finite ring extension of finite exponent whose modules of principal parts are projective is purely inseparable.

Proposition 3.46. *Let $A \subseteq C$ be a finite ring extension of finite exponent. If the C-module $\mathrm{P}^{p^e}_{C/A}$ is projective for all $0 \leq e < \exp(C/A)$, then $A \subseteq C$ is purely inseparable.*

Proof. There is nothing to prove in the trivial case. Hence, we assume that $\exp(C/A) \geq 1$ and that $\mathrm{P}^{p^e}_{C/A}$ is a projective C-module for all $0 \leq e < \exp(C/A)$. We proceed by induction on the exponent of the extension.

We claim that $\Omega_{C/A}$ is a projective C-module. Let J be the kernel of the multiplication map $C \otimes_A C \to C$ as in discussion 3.31. We have a decomposition $C \otimes_A C = C \oplus J$, that induces the next equality

$$\mathrm{P}^1_{C/A} = (C \otimes_A C)/J^2 = C \oplus (J/J^2) = C \oplus \Omega_{C/A}.$$

Then $\Omega_{C/A}$ is a direct summand of the projective module $\mathrm{P}^1_{C/A}$, so it is also projective (Proposition 1.2). Moreover, since $\Omega_{C/C^{[1]}} = \Omega_{C/A}$ and $C^{[1]} \subseteq C$ is a finite extension, we conclude that $C^{[1]} \subseteq C$ is Galois (Theorem 2.71). In particular, in the case

$\exp(C/A) = 1$ we have $C^{[1]} = A$, and this proves that $A \subseteq C$ is Galois, or equivalently, purely inseparable of exponent one (Theorem 2.71).

Thus, we suppose that $\exp(C/A) > 1$. Recall that $\exp(C^{[1]}/A) = \exp(C/A) - 1$. We first prove that $\mathrm{P}^{p^e}_{C^{[1]}/A}$ is a projective $C^{[1]}$-module for $0 \leq e < \exp(C^{[1]}/A)$ to apply later the inductive hypothesis. We already know that $C^{[1]} \subset C$ is Galois. Since $\mathrm{Spec}(A)$ and $\mathrm{Spec}(C^{[1]})$ are homeomorphic (Remark 2.2), there are elements $f_1, \ldots, f_r \in A$ generating the unit ideal such that C_{f_i} has a p-basis over $C^{[1]}_{f_i}$ by Proposition 2.55. Then, by Proposition 3.45, the natural map

$$C \otimes_{C^{[1]}} P^{p^e}_{C^{[1]}/A} \to P^{p^{e+1}}_{C/A}$$

has locally a retraction of C_{f_i}-modules. Since this occurs at each open subset of the covering generated by $f_1, \ldots, f_r \in A$, we have a global retraction of C-modules. By Lemma A.10, this implies that $C \otimes_{C^{[1]}} P^{p^e}_{C^{[1]}/A}$ is a C-module direct summand of $P^{p^{e+1}}_{C/A}$. This module is projective by hypothesis, so $C \otimes_{C^{[1]}} P^{p^e}_{C^{[1]}/A}$ is also projective (Proposition 1.2). Since $C^{[1]} \to C$ is faithfully flat (Remark 1.16), we conclude that $P^{p^e}_{C^{[1]}/A}$ is a projective $C^{[1]}$-module for all $0 \leq e < \exp(C^{[1]}/A)$ (Proposition 1.4.(2)). In this situation, we can apply the inductive hypothesis to deduce that $A \subset C^{[1]}$ is purely inseparable. Since $C^{[1]} \subset C$ is Galois, it follows that $A \subset C$ is purely inseparable by Corollary 3.19. □

We turn now to the perspective of differential operators. Using Proposition 3.39 on extension of differential operators from the previous subsection, we prove that an $\mathcal{F}$-extension is purely inseparable if the modules of differential operators are direct summands of the module of endomorphisms. This result extends Proposition 2.67 for Galois extensions of exponent one to purely inseparable ring extensions of higher exponent.

Proposition 3.47. *Let $A \subseteq C$ be an $\mathcal{F}$-extension such that $\mathrm{Diff}^{p^e}_A(C)$ is a C-module direct summand of $\mathrm{End}_A(C)$ for all $0 \leq e < \exp(C/A)$. Then $A \subseteq C$ is purely inseparable.*

Proof. The case of trivial extensions is clear, so we suppose $\exp(C/A) \geq 1$. We proceed by induction on the exponent. Note that the exponent one case was already settled in Proposition 2.67. Indeed, our hypothesis are that C is a projective A-module and that $\mathrm{Diff}^1_A(C) = C \oplus \mathrm{Der}_A(C)$ is a C-module direct summand of $\mathrm{End}_A(C)$. Since $\mathrm{Diff}^1_A(C) = C \oplus \mathrm{Der}_A(C)$ (see (6) in discussion 3.30), the latter implies that $\mathrm{Der}_A(C)$ is a C-module direct summand of $\mathrm{End}_A(C)$ too.

Assume now that $\exp(C/A) > 1$. We will reduce the proof to the setting of local rings. Since $A \subset C$ is an $\mathcal{F}$-extension, then C is a finite projective A-module (Lemma 3.24). Thus, it only lefts to prove that the extension $A_{\mathfrak{p}} \subset C_{\mathfrak{p}}$ is purely inseparable for each prime ideal $\mathfrak{p} \subset A$. Note that C has finite presentation over A as it is a projective module (Proposition 1.7), so

$$(\mathrm{End}_A(C))_{\mathfrak{p}} = \mathrm{End}_{A_{\mathfrak{p}}}(C_{\mathfrak{p}}) \quad \text{and} \quad (\mathrm{Diff}^{p^e}_A(C))_{\mathfrak{p}} = \mathrm{Diff}^{p^e}_{A_{\mathfrak{p}}}(C_{\mathfrak{p}})$$

by Corollary 1.25 and Corollary 3.35) respectively. The hypothesis implies that $\mathrm{Diff}^{p^e}_{A_{\mathfrak{p}}}(C_{\mathfrak{p}})$ is a $C_{\mathfrak{p}}$-direct summand of $\mathrm{End}_{A_{\mathfrak{p}}}(C_{\mathfrak{p}})$, since localization commutes with direct sum. By Remark 3.23, we also know that $A_{\mathfrak{p}} \subset C_{\mathfrak{p}}$ is an $\mathcal{F}$-extension. Therefore, we can assume that A is local for the rest of the proof. Hence, C and $C^{[e]}$ are also local for all $e \geq 0$ (Remark 2.2).

Recall that the extension $A \subset C$ is purely inseparable if and only if $A \subset C^{[1]}$ is purely inseparable and $C^{[1]} \subset C$ is Galois (Corollary 3.19). We prove first that $C^{[1]} \subset C$ is a Galois extension. Observe that C is a projective $C^{[1]}$-module, because $A \subset C$ is an $\mathcal{F}$-extension (Lemma 3.24). We consider the following tower of C-modules

$$\mathrm{Diff}^1_A(C) = \mathrm{Diff}^1_{C^{[1]}}(C) \subseteq \mathrm{End}_{C^{[1]}}(C) \subseteq \mathrm{End}_A(C).$$

Note that $\mathrm{Diff}^1_A(C)$ is a C-module direct summand of $\mathrm{End}_A(C)$ by hypothesis and that $\mathrm{End}_{C^{[1]}}(C)$ is a C-module direct summand of $\mathrm{End}_A(C)$, since C is a projective $C^{[1]}$-module (Proposition 1.26). Therefore, $\mathrm{Diff}^1_{C^{[1]}}(C)$ is a C-module direct summand of $\mathrm{End}_{C^{[1]}}(C)$. By the exponent one case, $C^{[1]} \subset C$ is Galois.

We now prove that $A \subset C^{[1]}$ is purely inseparable. Since we have $\exp(C^{[1]}/A) = \exp(C/A) - 1$, it is enough to show that $A \subset C^{[1]}$ satisfies the hypothesis on the statement and apply the inductive hypothesis. It is clear that $A \subset C^{[1]}$ is an $\mathcal{F}$-extension, since so is $A \subset C$ (see Remark 3.22). Hence, it only lefts to prove that $\mathrm{Diff}^{p^e}_A(C^{[1]})$ is a $C^{[1]}$-direct summand of $\mathrm{End}_A(C^{[1]})$ for all $0 \leq e < \exp(C^{[1]}/A)$. We consider the following commutative diagram

$$\begin{array}{ccccc}
 & \overset{\mathrm{ext}}{\curvearrowleft} & & \overset{\Phi}{\curvearrowright} & \\
\mathrm{End}_A(C) & \xrightarrow{\mathrm{res}} & \mathrm{Hom}_A(C^{[1]}, C) & \hookleftarrow & \mathrm{End}_A(C^{[1]}) \\
\uparrow \Phi \downarrow & & \uparrow & & \uparrow \\
 & \underset{\mathrm{ext}}{\curvearrowleft} & & \underset{\Phi}{\curvearrowright} & \\
\mathrm{Diff}^{p^{e+1}}_A(C) & \xrightarrow{\mathrm{res}} & \mathrm{Diff}^{p^e}_A(C^{[1]}, C) & \hookleftarrow & \mathrm{Diff}^{p^e}_A(C^{[1]}),
\end{array}$$

where res denotes the restriction maps as in Proposition 3.38, ext is the extension map defined in Proposition 3.39 and the unnamed maps are natural inclusions. We show that each map Φ is a retraction to the corresponding inclusion. On the one hand, the existence of the vertical retraction $\Phi\colon \mathrm{End}_A(C) \to \mathrm{Diff}^{p^{e+1}}_A(C)$ on the left of the diagram follows from the hypothesis that $\mathrm{Diff}^{p^{e+1}}_A(C)$ is a C-module direct summand of $\mathrm{End}_A(C)$ (see Lemma A.10). On the other hand, the existence of the horizontal retraction maps can be justified as follows. Since we have proved that $C^{[1]} \subset C$ is a Galois extension between local rings, C has a p-basis $\{x_1, \ldots, x_n\}$ over $C^{[1]}$ and the reduced monomials $\mathbf{x}^\alpha$ form a basis for C as $C^{[1]}$-module. Then there is a natural homomorphism of $C^{[1]}$-modules $C \to C^{[1]}$ given by $\sum c_\alpha \mathbf{x}^\alpha \mapsto c_0$, which is a retraction to the inclusion $C^{[1]} \hookrightarrow C$. Note that it induces retractions $\Phi\colon \mathrm{Hom}_A(C^{[1]}, C) \to \mathrm{End}_A(C^{[1]})$ and $\Phi\colon \mathrm{Diff}^{p^e}_A(C^{[1]}, C) \to \mathrm{Diff}^{p^e}_A(C^{[1]})$ to the reverse inclusions.

All the maps in the above diagram are morphisms of $C^{[1]}$-modules. Then, following the arrows in the commutative diagram, we see that the map $\mathrm{End}_A(C^{[1]}) \to$

$\mathrm{Diff}_A^{p^e}(C^{[1]})$, deduced from the composition of the maps in the diagram, is a retraction of the reverse inclusion. Thus, by Lemma A.10, we conclude that $\mathrm{Diff}_A^{p^e}(C^{[1]})$ is a $C^{[1]}$-direct summand of $\mathrm{End}_A(C^{[1]})$.

We have shown that the extension $A \subset C^{[1]}$ satisfy the hypothesis in the statement. Therefore, $A \subset C^{[1]}$ is purely inseparable by the inductive hypothesis, and this completes the proof. □

To sum up, as a consequence of the results in this section, we obtain the next characterizations of purely inseparable extensions of rings in terms of differential operators and modules of principal parts. It extends in some sense the equivalence (1) ⇔ (6) from Theorem 2.71 for exponent one extensions to the higher exponent setting.

Theorem 3.48. *Let $A \subseteq C$ be a finite ring extension of finite exponent. Then the following conditions are equivalent.*

(1) $A \subseteq C$ is purely inseparable.

(2) $\mathrm{P}^k_{C/A}$ is a projective C-module for all $k \geq 0$.

(3) $\mathrm{P}^{p^e}_{C/A}$ is projective C-module for all $0 \leq e < \exp(C/A)$.

(4) $A \subseteq C$ is an $\mathcal{F}$-extension and $\mathrm{Diff}^k_A(C)$ is a C-direct summand of $\mathrm{End}_A(C)$ for all $k \geq 0$.

(5) $A \subseteq C$ is an $\mathcal{F}$-extension and $\mathrm{Diff}^{p^e}_A(C)$ is a C-direct summand of $\mathrm{End}_A(C)$ for all $0 \leq e < \exp(C/A)$.

Proof. The implications (1)⇒(2) and (1)⇒(4) are set out in Proposition 3.43. It is clear that (2) implies (3) and that (4) implies (5). Proposition 3.46 establishes that (3)⇒(1) and the implication (5)⇒(1) is proved in Proposition 3.47. □

We note that the above theorem includes the characterization of purely inseparable extensions given by P.J. Sancho de Salas in [56, Theorem 3.8]. However, we approach the characterization from a completely different perspective.

3.3. Towers of purely inseparable extensions

The setting for this section are rings of prime characteristic p. We study towers of purely inseparable extensions following our approach in [11, §6], which is joint work of the author of this thesis with D. Sulca. We begin by introducing the definition of purely inseparable tower of rings.

Definition 3.49. A tower of rings $A \subseteq B \subseteq C$ is a *purely inseparable tower* if $A \subseteq C$, $A \subseteq B$ and $B \subseteq C$ are purely inseparable extensions. Note that if $A \subseteq C$ has exponent one, a purely inseparable tower of rings is exactly a *Galois tower* (see Definition 2.72).

Remark 3.50. Observe that if $A \subseteq B$ and $B \subseteq C$ have finite exponent, then $A \subseteq C$ has also finite exponent. The converse is also true. More precisely,

$$\max\{\exp(B/A), \exp(C/B)\} \leq \exp(C/A) \leq \exp(B/A) + \exp(C/B).$$

This section deals with two questions regarding purely inseparable towers of rings. We will use the notion of $\mathcal{F}$-extension, introduced in the previous sections (see Definition 3.21), to give some answers to the following questions. In Subsection 3.3.1, we consider the problem of characterizing those intermediate subrings B of a purely inseparable extension of rings $A \subseteq C$ such that $A \subseteq B$ and $B \subseteq C$ are also purely inseparable, that is, those subrings such that $A \subseteq B \subseteq C$ is a purely inseparable tower of rings. In Subsection 3.3.2, we study when the composition of two purely inseparable extensions of rings $A \subseteq B$ and $B \subseteq C$ gives a purely inseparable tower $A \subseteq B \subseteq C$.

3.3.1. Intermediate subrings of a purely inseparable ring extension

In this subsection, we look for conditions for intermediate subrings B of a purely inseparable extension of rings $A \subseteq C$ that guarantee that $A \subseteq B \subseteq C$ is a purely inseparable tower. The situation is well understood when $A \subseteq C$ has exponent at most one, while the problem remains open if the extension has exponent greater than one.

However, we show some sufficient conditions that ensure that $A \subseteq B \subseteq C$ is a purely inseparable extension for a given purely inseparable extension $A \subseteq C$ of finite exponent and an intermediate subring B. More precisely, we show that if B is an intermediate subring of a purely inseparable extension $A \subseteq C$ such that $A \subseteq B$, $B \subseteq C$ and $A \subseteq B[C^{p^k}]$ are $\mathcal{F}$-extensions for $1 \leq k < \exp(C/B)$, then $A \subseteq B \subseteq C$ is a purely inseparable tower (Proposition 3.54). In fact, for exponent two extensions, the condition on $A \subseteq B[C^{p^k}]$ can be omitted, so we obtain a characterization for purely inseparable towers in this case.

We begin by reviewing the situation for exponent one extensions. As we have discussed in Section 2.3 from the second chapter, S. Yuan proved that if $A \subseteq C$ is Galois and B is an intermediate subring such that $B \subseteq C$ is also Galois, then $A \subseteq B$ is automatically Galois ([68, Theorem 11]). Furthermore, M. André proved that an intermediate subring B defines a Galois tower $A \subseteq B \subseteq C$ if and only if C is a projective B-module (Proposition 2.73). Nevertheless, we can easily find examples $A \subseteq B \subseteq C$ where $A \subseteq C$ and $A \subseteq B$ are Galois but $B \subseteq C$ is not.

Example 3.51. Let $A = K$ be a field of characteristic $p = 2$. We consider the ring

$$C := K[X, Y]/\langle X^2, Y^2\rangle = K[x, y],$$

which is a purely inseparable extension of exponent one over A, with p-basis $\{x, y\}$, so $K \subset C$ is a Galois extension (see Lemma 2.45.(1)). We define the subring $B := K[xy] \subset K[x, y] = C$. Note that B is a free K-module of rank 2 and $\{xy\}$ is a p-basis, so $K \subset B$ is a Galois extension (see Lemma 2.45.(1) again). We show that $B \subset C$ is

not Galois by showing that C is not a flat B-module. Assume on the contrary that C is a flat B-module. Observe that $C/\langle xy\rangle = K[X,Y]/\langle X^2, XY, Y^2\rangle$ has a basis over $B/\langle xy\rangle = K$ induced by $\{1, x, y\}$. Since B is a local ring, if C were flat over B, then C would be a free B-module with basis $\{1, x, y\}$ as a consequence of Nakayama's Lemma (see Proposition A.36). But this is impossible since $(xy)x = 0$ in C. Hence, C is not a flat B-module. In particular, C is not projective as B-module, and therefore it is not a Galois extension by Proposition 2.73.

We focus now on purely inseparable extensions of higher exponent. We observe that the characterization of Galois towers from Proposition 2.73 does not hold for purely inseparable extensions of exponent greater than one. Indeed, the next example shows a tower of rings $A \subseteq B \subseteq C$ where $A \subseteq C$ is a purely inseparable ring extension of exponent two, $B \subseteq C$ is a Galois extension, but $A \subseteq B$ is not purely inseparable.

Example 3.52. Let $A = K$ be a field of characteristic $p = 3$. We set

$$B := K[X, Y, Z_1, Z_2]/\langle X^3, Y^3, Z_1^3 - X^2, Z_2^3 - Y^2\rangle = K[x, y, z_1, z_2],$$

which is an extension of A of exponent 2. We set

$$C := B[T_1, T_2]/\langle T_1^3 - x, T_2^3 - y\rangle = K[x, y, z_1, z_2, t_1, t_2].$$

By definition C admits $\{t_1, t_2\}$ as a p-basis over B, so $B \subset C$ is a Galois extension by Lemma 2.45.(1). Note also that the extension $A \subset C$ has exponent 2. We show that $A \subset C$ is purely inseparable. Indeed, by Theorem 3.18 it is enough to show that $A \subset A[C^3]$ and $A[C^3] \subset C$ are Galois. Note that $A[C^3] = K[x, y]$ is a Galois extension over A with p-basis $\{x, y\}$, and

$$C = A[C^3][Z_1, Z_2, T_1, T_2]/\langle Z_1^3 - x^2, Z_2^3 - y^2, T_1^3 - x, T_2^3 - y\rangle$$

is Galois over $A[C^3]$ with p-basis $\{z_1, z_2, t_1, t_2\}$. We finally show that $A \subset B$ is not purely inseparable. By Theorem 3.18, it is enough to show that $A \subset A[B^3]$ is not Galois. Since A is local, this is the same to show that $A[B^3]$ does not admit a p-basis over A. Note that $A[B^3] = K[x^2, y^2]$ has a basis over K with four elements, namely, the monomials $1, x^2, y^2, (xy)^2$. Then $A[B^3]$ has rank equal to four over A, which is not a power of $p = 3$. But if $A \subset A[B^3]$ had a p-basis, it would necessarily have rank a power of $p = 3$ (see Remark 2.23).

The next lemma extends in some sense Proposition 2.73 for exponent one ring extensions to the higher exponent case.

Lemma 3.53. *Let $A \subseteq C$ be a purely inseparable ring extension and let B be an intermediate subring, $A \subseteq B \subseteq C$, such that $A \subseteq B$ and $B \subseteq C$ are $\mathcal{F}$-extensions. If $B \subseteq C$ has exponent at most one, then $A \subseteq B$ is purely inseparable and $B \subseteq C$ is Galois.*

Proof. If $A = C$ or $B = C$, the result is trivial, so we assume that $\exp(C/A) \geq 1$ and $\exp(C/B) = 1$. We proceed by induction on the exponent of $A \subseteq C$. If $\exp(C/A) = 1$,

the lemma reduces to Proposition 2.73, because C is a projective B-module as $B \subset C$ is an $\mathcal{F}$-extension (see Lemma 3.24).

Suppose now that $\exp(C/A) > 1$. We first prove that $B \subset C$ is Galois. Since $\exp(C/B) = 1$, we have $C^p \subseteq B$ and we can consider the tower

$$A[C^p] \subseteq B \subset C.$$

Note that $A[C^p] \subset C$ is Galois, because $A \subset C$ is purely inseparable (see Corollary 3.19). In addition, C is a projective B-module by Lemma 3.24. Thus, both $A[C^p] \subseteq B$ and $B \subset C$ are Galois by Proposition 2.73.

We prove now that $A \subseteq B$ is purely inseparable. By Corollary 3.19, this follows if we show that $A \subseteq A[B^p]$ is purely inseparable and $A[B^p] \subseteq B$ is Galois. In order to prove that $A \subseteq A[B^p]$ is purely inseparable, we show that the tower of rings

$$A \subseteq A[B^p] \subset A[C^p]$$

satisfies the hypothesis of the lemma. Note that the extension $A \subset A[C^p]$ is purely inseparable of exponent $\exp(C/A) - 1$ (see Corollary 3.19) and that $A \subseteq A[B^p]$ is an $\mathcal{F}$-extension, because so is $A \subseteq B$ (see Remark 3.22). Then it only lefts to check that $A[B^p] \subset A[C^p]$ is an $\mathcal{F}$-extension of exponent at most one. In fact, $A[B^p] \subset A[C^p]$ has exponent at most one, since $(A[C^p])^p \subseteq (A[B])^p \subseteq A[B^p]$ as $C^p \subseteq B$. Moreover, $A[B^p] \subset A[C^p]$ is an $\mathcal{F}$-extension if and only if $A[C^p]$ is a projective $A[B^p]$-module. So we prove the last condition. Observe that C is a projective B-module and B is a projective $A[B^p]$-module by hypothesis, because $B \subseteq C$ and $A \subseteq B$ are $\mathcal{F}$-extensions respectively (Lemma 3.24). Hence, C is a projective $A[B^p]$-module by Proposition 1.5. In addition, we know that C is a projective $A[C^p]$-module, because the extension $A[C^p] \subset C$ is Galois. Therefore, $A[C^p]$ is a projective $A[B^p]$-module, by considering the tower $A[B^p] \subset A[C^p] \subset C$ in Lemma 1.17.

Since $A \subset A[C^p]$ has exponent smaller than $\exp(C/A)$ and we have proved that $A \subseteq A[B^p] \subset A[C^p]$ satisfies the hypothesis in the statement, we can apply the inductive hypothesis to deduce that $A \subseteq A[B^p]$ is purely inseparable and $A[B^p] \subset A[C^p]$ is Galois. It only lefts to show that $A[B^p] \subseteq B$ is Galois. We consider the tower of rings

$$A[B^p] \subset A[C^p] \subseteq B.$$

We have just proved that $A[B^p] \subset A[C^p]$ is Galois, and we have also proved that $A[C^p] \subseteq B$ is Galois in the second paragraph. Therefore, since $A[B^p] \subset B$ has exponent at most one, we conclude that $A[B^p] \subset B$ is Galois by Lemma 2.45.(3).

In summary, we have proved that $A \subseteq A[B^p]$ is purely inseparable and $A[B^p] \subset B$ is Galois. Hence, $A \subset B$ is a purely inseparable extension by Corollary 3.19. As we proved at the beginning that $B \subset C$ is Galois, the proof of the lemma is complete. □

We use the above lemma to give sufficient conditions for an intermediate subring of a purely inseparable extension to induce a purely inseparable tower of rings.

Proposition 3.54. *Let $A \subseteq C$ be a purely inseparable extension and let B be an intermediate subring, $A \subseteq B \subseteq C$. Assume that the following conditions hold:*

(1) $A \subseteq B$ *is an* $\mathcal{F}$*-extension;*

(2) $B \subseteq C$ *is an* $\mathcal{F}$*-extension; and*

(3) $A \subseteq B[C^{p^k}]$ *is an* $\mathcal{F}$*-extension for all* $1 \leq k < \exp(C/B)$.

Then $A \subseteq B \subseteq C$ *is a purely inseparable tower. Moreover,* $A \subseteq B[C^{p^k}] \subseteq C$ *is also a purely inseparable tower for all* $1 \leq k < \exp(C/B)$.

Proof. We prove that $A \subseteq B[C^{p^k}] \subseteq C$ is a purely inseparable tower by induction in $k \geq 0$. In particular, when $k = \exp(C/B)$, we have $B[C^{p^k}] = B$ and the previous condition will imply that $A \subseteq B \subseteq C$ is also a purely inseparable tower.

If $k = 0$, then $B[C^{p^k}] = C$ and the result is trivial, since $A \subseteq C$ is purely inseparable by hypothesis. For $k \geq 1$, we assume that $A \subseteq B[C^{p^{k-1}}] \subseteq C$ is a purely inseparable tower and we have to prove that the tower $A \subseteq B[C^{p^k}] \subseteq C$ is also purely inseparable. We first show that $A \subseteq B[C^{p^k}]$ is purely inseparable. For this, we consider the tower of rings

$$A \subseteq B[C^{p^k}] \subseteq B[C^{p^{k-1}}].$$

We show that this tower satisfies the conditions from Lemma 3.53. Note that $A \subseteq B[C^{p^{k-1}}]$ is purely inseparable by inductive hypothesis. Observe also that $A \subseteq B[C^{p^k}]$ is an $\mathcal{F}$-extension by assumption. In addition, $B[C^{p^k}] \subseteq B[C^{p^{k-1}}]$ is an extension of exponent at most one such that $B[C^{p^{k-1}}]$ is projective as $B[C^{p^k}]$-module, because $B \subseteq C$ is an $\mathcal{F}$-extension. Therefore, we can apply Lemma 3.53 to conclude that $A \subseteq B[C^{p^k}]$ is purely inseparable and $B[C^{p^k}] \subseteq B[C^{p^{k-1}}]$ is Galois.

Hence, it only lefts to show that $B[C^{p^k}] \subseteq B$ is purely inseparable. We have already proved that $B[C^{p^k}] \subseteq B[C^{p^{k-1}}]$ is Galois and $B[C^{p^{k-1}}] \subseteq C$ is purely inseparable by the inductive hypothesis. Then we conclude that $B[C^{p^k}] \subseteq C$ is purely inseparable by Theorem 3.18. This completes the induction. □

In the setting of the previous proposition, if the extension $A \subseteq C$ has exponent at most one, then the conditions (1) and (3) are a consequence of condition (2) (see Proposition 2.73). Furthermore, we will show in the next result that if the exponent of the extension is two, then conditions (1) and (2) imply condition (3). This leads us to the following characterization for purely inseparable towers of exponent two.

Corollary 3.55. *Let* $A \subseteq C$ *be a purely inseparable extension of exponent two and let* B *be an intermediate subring,* $A \subseteq B \subseteq C$*. Then* $A \subseteq B \subseteq C$ *is a purely inseparable tower if and only if* $A \subseteq B$ *and* $B \subseteq C$ *are* $\mathcal{F}$*-extensions.*

Proof. If $A \subseteq B \subseteq C$ is a purely inseparable tower, then it is clear that both $A \subseteq B$ and $B \subseteq C$ are $\mathcal{F}$-extensions. We prove the converse. Observe that $\exp(C/B) \leq 2$, as we noted in Remark 3.50. Then, by Proposition 3.54, we only have to check that $A \subseteq B[C^p]$ is an $\mathcal{F}$-extension. Note that $A[(B[C^p])^p] = A[B^p]$, so, equivalently, we

have to show $B[C^p]$ is a projective $A[B^p]$-module and that $A[B^p]$ is a projective A-module. It is clear that the last condition holds because $A \subseteq B$ is an $\mathcal{F}$-extension (Lemma 3.24). So we consider the tower of rings $A[B^p] \subseteq B[C^p] \subseteq B$ to prove the former. We know that B is projective over $B[C^p]$, since $B \subseteq C$ is an $\mathcal{F}$-extension (Lemma 3.24), and it is also projective over $A[B^p]$, as we noted before. Therefore, considering the tower $A[B^p] \subseteq B[C^p] \subseteq B$, we deduce that $B[C^p]$ is a projective $A[B^p]$-module by Lemma 1.17, as we wanted. □

A similar argument to the one used in the proof of the above corollary can be used to refine Proposition 3.54 for purely inseparable ring extensions of exponent greater than two, as we show in the next proposition

Proposition 3.56. *Let $A \subseteq C$ be a purely inseparable extension of exponent greater than two. Let B be an intermediate subring, $A \subseteq B \subseteq C$, such that $A \subseteq B$ and $B \subseteq C$ are both $\mathcal{F}$-extensions. If $A \subseteq B[C^{p^k}]$ is an $\mathcal{F}$-extension for all $1 \leq k \leq \exp(C/A)-2$, then $A \subseteq B \subseteq C$ is a purely inseparable tower.*

Proof. Denote $e := \exp(C/A)$. By Proposition 3.54, the result holds if we show that $A \subseteq B[C^{p^{e-1}}]$ is also an $\mathcal{F}$-extension. We first note that $A[(B[C^{p^{e-1}}])^{p^k}] = A[B^{p^k}]$ for all $k \geq 1$. Therefore, we have to show that $B[C^{p^{e-1}}]$ is projective over $A[B^p]$ and that $A[B^{p^k}]$ is projective over $A[B^{p^{k+1}}]$ for all $k \geq 1$. Note that the last condition is true because $A \subseteq B$ is an $\mathcal{F}$-extension. To prove that $B[C^{p^{e-1}}]$ is a projective $A[B^p]$-module, we consider the next tower of rings

$$A[B^p] \subseteq B \subseteq B[C^{p^{e-1}}].$$

By Lemma 3.24, we have that $B[C^{p^{e-1}}]$ is a projective B-module, because $B \subseteq C$ is an $\mathcal{F}$-extension and that B is a projective $A[B^p]$-module, because $A \subseteq B$ is an $\mathcal{F}$-extension. Thus, $B[C^{p^{e-1}}]$ is a projective $A[B^p]$- module by Proposition 1.5, and this completes the proof. □

Remark 3.57. If $A \subseteq B \subseteq C$ is a purely inseparable tower and $A \subseteq B$ has exponent one, then we will show that $A \subseteq B[C^{p^k}]$ is an $\mathcal{F}$-extension for all k in Proposition 3.61 below. However, we do not know if the same is true when $A \subseteq B$ has exponent greater than one.

3.3.2. Composition of purely inseparable extensions of rings

Given a tower of rings $A \subseteq B \subseteq C$ with $A \subseteq B$ and $B \subseteq C$ purely inseparable, we consider in this subsection the problem of whether $A \subseteq C$ is also purely inseparable, that is, whether $A \subseteq B \subseteq C$ is a purely inseparable tower. As we will see, in general we need to add some extra conditions to reach this conclusion.

We begin by analysing the mentioned problem in the exponent one case. Let $A \subseteq B$ and $B \subseteq C$ be Galois extensions of exponent one. Then $A \subseteq C$ has exponent at most two (see Remark 3.50). If $A \subseteq C$ has exponent at most one, then it is Galois as we noted in Lemma 2.45.(3). However, if $A \subset C$ has exponent two, we cannot assure in general that $A \subset C$ is purely inseparable, as the following example shows.

Example 3.58. Let $A = K$ be a field of characteristic $p = 3$. We define the ring

$$B := K[X, Y]/\langle X^3, Y^3\rangle = K[x, y].$$

It is clear that $A \subset B$ is a Galois extension with p-basis $\{x, y\}$. Now we define the ring

$$C := B[Z_1, Z_2, Z_3]/\langle Z_1^3 - x^2, Z_2^3 - xy, Z_3^3 - y^2\rangle = K[x, y, z_1, z_2, z_3].$$

Then the extension $B \subset C$ is Galois with p-basis $\{z_1, z_2, z_3\}$. Note that $A[C^3] = K[x^2, xy, y^2] \subset K[x, y] = B$. One can easily check that $A[C^3]$ is a free A-module with a basis formed by the monomials $1, x^2, xy, y^2, (xy)^2$. Thus, $A \subset A[C^3]$ is an exponent one extension such that $A[C^3]$ has rank 5 over A. Since we are in the local case, if $A \subset A[C^3]$ were Galois, then $A[C^3]$ would be free of rank a power of 3 (see Remark 2.23). Since 5 is not a power of 3, $A \subset A[C^3]$ is not Galois. Therefore, by Theorem 3.18, $A \subset C$ is not purely inseparable.

In the next lemma, we give a characterization of purely inseparable ring extensions, which result from the composition of two Galois extensions.

Lemma 3.59. *Let $A \subseteq B$ and $B \subseteq C$ be Galois extensions of rings. Then $A \subseteq C$ is purely inseparable if and only if $A \subseteq C$ is an $\mathcal{F}$-extension. Moreover, in this case, $A[C^p] \subseteq B$ is also a Galois extension.*

Proof. If $A \subseteq C$ is purely inseparable, then it is in particular an $\mathcal{F}$-extension. We show that $A[C^p] \subseteq B$ is a Galois extension. We consider the tower $A[C^p] \subseteq B \subseteq C$. Note that $A[C^p] \subseteq C$ is Galois by Theorem 3.18 and that $B \subseteq C$ is Galois by hypothesis. Hence $A[C^p] \subseteq B$ is also Galois by Proposition 2.73.

Assume now that $A \subseteq B$ and $B \subseteq C$ are Galois extension and that $A \subseteq C$ is an $\mathcal{F}$-extension. We have to prove that $A \subseteq C$ is purely inseparable. By Remark 3.50, we know that $\exp(C/A) \leq 2$. Thus, it is sufficient to prove that $A \subseteq A[C^p]$ and $A[C^p] \subseteq C$ are Galois by Corollary 3.19. With this aim, we consider first the tower

$$A[C^p] \subseteq B \subseteq C.$$

Note that C is projective as B-module, because $B \subseteq C$ is Galois, and it is also projective as $A[C^p]$-module, because $A \subseteq C$ is an $\mathcal{F}$-extension (Lemma 3.24). Hence, B is a projective $A[C^p]$-module by Lemma 1.17. We consider now the tower

$$A \subseteq A[C^p] \subseteq B.$$

Since $A \subseteq B$ is Galois and B is a projective $A[C^p]$-module, both extensions $A \subseteq A[C^p]$ and $A[C^p] \subseteq B$ are Galois by Proposition 2.73. Finally, using that $A[C^p] \subseteq B$ and $B \subseteq C$ are Galois and that $A[C^p] \subseteq C$ has exponent at most one, we conclude that $A[C^p] \subseteq C$ is Galois by Lemma 2.45.(3). □

In the above lemma, we have shown that the composition of two Galois extensions is Galois if and only if it is an $\mathcal{F}$-extension. We now turn to the study of a more general case. In the next propositions, we characterize the compositions of a purely inseparable extension of higher exponent with a Galois extension.

Proposition 3.60. *Let $A \subseteq B \subseteq C$ be a tower of ring extensions such that $A \subseteq B$ is purely inseparable and $B \subseteq C$ is Galois. Then $A \subseteq C$ is purely inseparable if and only if $A \subseteq C$ is an $\mathcal{F}$-extension.*

Proof. If $A \subseteq C$ is purely inseparable, we already know that $A \subseteq C$ is an $\mathcal{F}$-extension.

Conversely, assume that $A \subseteq C$ is an $\mathcal{F}$-extension. We have to show that $A \subseteq C$ is purely inseparable. By Corollary 3.19, this is equivalent to show that $A \subseteq A[C^p]$ is purely inseparable and $A[C^p] \subseteq C$ is Galois. We first prove that $A \subseteq A[C^p]$ is purely inseparable. We consider the tower of rings

$$A \subseteq A[C^p] \subseteq B.$$

We show that it satisfies the assumptions from Lemma 3.53. By hypothesis $A \subseteq B$ is purely inseparable, and $A \subseteq A[C^p]$ is an $\mathcal{F}$-extension (Remark 3.22). In addition, C is projective as $A[C^p]$-module, because $A \subseteq C$ is an $\mathcal{F}$-extension (Lemma 3.24), and it is also projective as B-module, because $B \subseteq C$ is Galois. Thus, considering the tower $A[C^p] \subseteq B \subseteq C$, it follows that B is a projective $A[C^p]$-module by Lemma 1.17. Hence, we can apply Lemma 3.53 to deduce that $A \subseteq A[C^p]$ is purely inseparable and $A[C^p] \subseteq B$ is Galois. Therefore, it only lefts to prove that $A[C^p] \subseteq C$ is Galois. We consider the tower of rings

$$A[C^p] \subseteq B \subseteq C.$$

We have proved that $A[C^p] \subseteq B$ is Galois and we also have that $B \subseteq C$ is Galois by hypothesis. Since $A[C^p] \subseteq C$ has exponent at most one, we conclude by Lemma 2.45.(3) that $A[C^p] \subseteq C$ is Galois. □

Proposition 3.61. *Let $A \subseteq B \subseteq C$ be a tower of ring extensions such that $A \subseteq B$ is Galois and $B \subseteq C$ is purely inseparable. Then $A \subseteq C$ is purely inseparable if and only if $A \subseteq C$ is an $\mathcal{F}$-extension. Moreover, in this case, each of the extensions $A \subseteq B[C^{p^k}]$ is purely inseparable for all $k \geq 1$.*

Proof. If $A \subseteq C$ is purely inseparable, then we know that $A \subseteq C$ is in particular an $\mathcal{F}$-extension. We now prove the converse. More generally, we prove by induction on $\exp(C/B)$ that if $A \subseteq C$ is an $\mathcal{F}$-extension then $A \subseteq B[C^{p^k}]$ is purely inseparable for all $k \geq 0$. Note that, for $k = 0$, this condition implies that $A \subseteq C$ is purely inseparable.

If $\exp(C/B) = 1$, the result coincides with Lemma 3.59. So we assume that $\exp(C/B) > 1$. We consider the tower of rings

$$A \subseteq B \subset B[C^p]$$

and show that it satisfies the hypothesis in the statement. Note that $A \subseteq B$ is Galois by assumption and that $B \subset B[C^p]$ is purely inseparable of exponent $\exp(C/B) - 1$ by Corollary 3.19. We have to verify that $A \subset B[C^p]$ is an $\mathcal{F}$-extension. For $k \geq 1$ we have $A[(B[C^p])^{p^k}] = A[C^{p^{k+1}}]$ since $A \subseteq B$ has exponent at most one. Since $A \subseteq C$ and $B \subset C$ are $\mathcal{F}$-extensions, we have that C is projective over $A[C^{p^{k+1}}]$ and also

over $B[C^p]$ by Lemma 3.24. Thus, considering the tower $A[C^{p^{k+1}}] \subseteq B[C^p] \subset C$, we deduce that $B[C^p]$ is projective over $A[C^{p^{k+1}}]$ by Lemma 1.17.

We can now apply the inductive hypothesis to the tower $A \subseteq B \subset B[C^p]$ and conclude that $A \subseteq B[C^{p^{k+1}}]$ is purely inseparable for all $k \geq 0$. Equivalently, $A \subseteq B[C^{p^k}]$ is purely inseparable for all $k \geq 1$. Hence, it only lefts to prove that $A \subset C$ is purely inseparable. We consider the tower

$$A \subset B[C^p] \subset C$$

where $A \subset B[C^p]$ is purely inseparable as we proved above, $B[C^p] \subset C$ is Galois (Corollary 3.19), and $A \subset C$ is an $\mathcal{F}$-extension by assumption. By Proposition 3.60, the composition $A \subset C$ is purely inseparable. Then we have shown that $A \subset B[C^{p^k}]$ is purely inseparable for all $k \geq 0$, as we wanted. □

Finally, as a corollary, we obtain that the composition of two purely inseparable extensions induces a purely inseparable tower if we ask some intermediate subextensions to be $\mathcal{F}$-extensions.

Corollary 3.62. *Let $A \subseteq B$ and $B \subseteq C$ be purely inseparable extensions of rings. If $A \subseteq B[C^{p^k}]$ is an $\mathcal{F}$-extension for all $k \geq 1$, then $A \subseteq C$ is purely inseparable.*

Proof. We prove the result using an inductive argument. Denote $e := \exp(C/B)$. Since $B \subseteq C$ is purely inseparable, for all $0 \leq k < e$, the intermediate subextensions $B[C^{p^{k+1}}] \subseteq B[C^{p^k}]$ are Galois (Theorem 3.18). We analyse the case in which $k = e-1$. We consider the next tower of rings

$$A \subseteq B \subseteq B[C^{p^{e-1}}]$$

and show that it satisfies the assumptions from Proposition 3.60. By hypothesis, $A \subseteq B$ is purely inseparable and $A \subseteq B[C^{p^{e-1}}]$ is an $\mathcal{F}$-extension. In addition, $B \subseteq B[C^{p^{e-1}}]$ is Galois, as we noted before. Thus, the extension $A \subseteq B[C^{p^{e-1}}]$ is purely inseparable by Proposition 3.60.

Using the same argument and descending on k, we may assume that $A \subseteq B[C^{p^{k+1}}]$ is purely inseparable for each $0 \leq k < e$. Then we consider the tower of rings

$$A \subseteq B[C^{p^{k+1}}] \subseteq B[C^{p^k}].$$

As we noted before, $B[C^{p^{k+1}}] \subseteq B[C^{p^k}]$ is Galois and $A \subseteq B[C^{p^k}]$ is an $\mathcal{F}$-extension, so $A \subseteq B[C^{p^k}]$ is purely inseparable by Proposition 3.60. In particular, when we reach $k = 0$, we conclude that $A \subseteq C$ is purely inseparable. □

CHAPTER 4
Modular extensions of rings

We dedicate this final chapter to the study of *modular extensions*. We will show that modular extensions are a subclass of purely inseparable extensions, already studied in Chapter 3. Namely, a modular extension of rings is a commutative ring extension with unity $A \subseteq C$ of prime characteristic p such that

(i) $C^{p^e} \subseteq A$ for some $e \geq 0$;

(ii) C is a finitely generated and projective A-module; and

(iii) for each prime ideal $\mathfrak{p} \subset A$, the corresponding $A_{\mathfrak{p}}$-algebra $C \otimes_A A_{\mathfrak{p}}$ is isomorphic to one of the form $A_{\mathfrak{p}}[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}} - a_1, \ldots, X_n^{p^{e_n}} - a_n \rangle$ for some $n \geq 0$, $e_i > 0$ and $a_i \in A_{\mathfrak{p}}$.

Note that if $A \subseteq C$ has exponent at most one, then the previous definition coincides with the definition of Galois extensions of rings, which is essentially a finite projective extension that admits locally, at each prime, a p-basis. A sequence of elements that induce a presentation as in (iii) will be called a *generalized p-basis*. This notion was introduced by S. Yuan in [67] in order to extend the notion of p-basis for exponent one extensions to the higher exponent setting. He proved that a finite projective ring extension $A \subseteq C$ of finite exponent, where A is a field, has a generalized p-basis if and only if $\mathrm{End}_A(C) = C[H]$ for some subset H of higher derivations such that $\ker(H) = A$. Equivalently, if and only if C is "differentiably simple" with respect to the set H of higher derivations.

However, our main interest is to understand modular extensions of rings as a subclass of purely inseparable extensions. We show that our definition of modular extension as a finite projective ring extension that locally admits a generalized p-basis generalizes the original definition of modular field extensions. In the setting of fields, these extensions were introduced by M. S. Sweedler ([62]). Indeed, he considered modular extensions to the purely inseparable theory what normal extensions are to separable theory. Modular field extensions have been widely studied ([22], [30], [42], [17], [64]).

Among the many characterizations of modular field extensions, M.S. Sweedler proves in [62, Theorem 1] that a purely inseparable field extension $K \subseteq L$ is modular

if and only if L^{p^e} and K are linearly disjoint over their intersection for all integer $e \geq 0$. Later, S. Satô uses this condition to define modularity for integral domain extensions ([58, Theorem 1]). We will extend this characterization to our definition of modular for ring extensions. More precisely, we will prove that a purely inseparable extension of rings is modular if and only if the subrings C^{p^e} and A are linearly disjoint over their intersection for all $e \geq 0$

Organization. This chapter is divided in two sections. The first one introduces some preliminaries that are needed in the subsequent section. The second one addresses modular ring extensions and its relation with linearly disjointedness. The contents from this chapter are unreleased results that come from discussions between the author of this thesis and D. Sulca.

Section 4.1 collects some preliminaries. We study the property of linearly disjointedness in the general setting of rings. We introduce a notion of generalized p-generating sequence and review the notion of generalized p-basis for finite extensions of arbitrary finite exponent, and some of its basic properties.

Section 4.2 gives a definition of modularity for finite ring extensions in general, that extends the classic notion for finite field extensions. We show that modular extensions are a subclass of purely inseparable (Proposition 4.33). Moreover, we prove that modular extensions are exactly those purely inseparable extensions $A \subseteq C$ such that C^{p^e} and A are linearly disjoint for all $e \geq 0$ (Theorem 4.38).

4.1. Preliminaries for modular extensions

We include in this section some basic concepts and results that are necessary to study modular extensions of rings. In Subsection 4.1.1, we revise linearly disjointedness for ring extensions in general and some properties under some conditions of finite projective modules. In Subsection 4.1.2, we introduce the notion of generalized p-generating sequences for finite extensions of finite exponent between local rings. Finally, in Subsection 4.1.3, we revise the concept of generalized p-basis and some of its basic properties.

4.1.1. Linearly disjointedness

In this subsection, we remain in the general setting of commutative rings with unity of any characteristic. We introduce linearly disjointedness for subrings of a given ring. This notion was originally formulated for subalgebras of a field extension. An introduction to this topic in the setting of fields can be found in [38, IV, §5]. We extend some of the results in there to the more general setting of subalgebras of a ring extension.

Definition 4.1. Let C be a ring, let A and B be subrings of C and let $R := A \cap B$. We denote by $A[B]$ or $B[A]$ the image of the natural map $A \otimes_R B \to C$ that sends $a \otimes b$ into ab. The rings A and B are *linearly disjoint* if this map is injective, equivalently, if $A \otimes_R B$ is naturally isomorphic to $A[B]$.

Remark 4.2. Note that A and B are linearly disjoint if and only if the following diagram is cartesian:

$$\begin{array}{ccc} A & \longrightarrow & A[B] \\ \uparrow & & \uparrow \\ R := A \cap B & \longrightarrow & B \end{array}$$

We show in the following lemma that the property of being linearly disjoint is a condition that can be checked locally at every prime ideal of the underlying intersection ring.

Lemma 4.3. *Let A and B be subrings of a ring C and let $R := A \cap B$. The following conditions are equivalent:*

(1) A and B are linearly disjoint.

(2) For each prime ideal $\mathfrak{p} \subset R$, the rings $A_{\mathfrak{p}}$ and $B_{\mathfrak{p}}$ are linearly disjoint (as subrings of $C_{\mathfrak{p}}$).

(3) For each maximal ideal $\mathfrak{m} \subset R$, the rings $A_{\mathfrak{m}}$ and $B_{\mathfrak{m}}$ are linearly disjoint (as subrings of $C_{\mathfrak{m}}$).

Proof. Let $\mathfrak{p} \subset R$ be any prime ideal. Since localization $R \to R_{\mathfrak{p}}$ commutes with tensor product, we have $(A \otimes_R B)_{\mathfrak{p}} = A_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} B_{\mathfrak{p}}$. In addition, as localization is flat, the exact sequence of R-modules,

$$0 \to A \cap B \to C \to C/A \oplus C/B \to 0,$$

remains exact after localizing at $\mathfrak{p}$, so $R_{\mathfrak{p}} = (A \cap B)_{\mathfrak{p}} = A_{\mathfrak{p}} \cap B_{\mathfrak{p}}$. Thus, the map $A_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} B_{\mathfrak{p}} \to C_{\mathfrak{p}}$ coincides with the map $(A \otimes_R B)_{\mathfrak{p}} \to C_{\mathfrak{p}}$. Therefore, the lemma follows from the fact that $A \otimes_R B \to C$ is injective if and only if $(A \otimes_R B)_{\mathfrak{p}} \to C_{\mathfrak{p}}$ is injective for every prime $\mathfrak{p} \subset A$ if and only if $(A \otimes_R C)_{\mathfrak{m}} \to C_{\mathfrak{m}}$ is injective for every maximal ideal $\mathfrak{m} \subset A$ (see Lemma A.9). □

We discuss in the next lemma the particular case in which one of the subrings A or B of the ring C is a free module over $R := A \cap B$. It will be very useful to prove later some properties on linearly disjointedness.

Lemma 4.4. *Let A and B be subrings of a ring C. Assume that B is a free module over $R := A \cap B$ with basis $\{b_i\}_{i \in I}$. Then A and B are linearly disjoint if and only if $A[B]$ is a free A-module with basis $\{b_i\}_{i \in I}$.*

Proof. Observe that $\{1 \otimes b_i\}$ is a basis for $A \otimes_R B$ as A-module. The natural map $A \otimes_R B \to A[B]$ is a surjective homomorphism of A-modules that sends $1 \otimes b_i$ into b_i. Hence, it is an isomorphism if and only if $\{b_i\}_{i \in I}$ is a basis of $A[B]$ over A. □

We establish now some results on linearly disjointedness that hold for some finite projective extensions of rings. The next lemma shows a sufficient condition for a pair of subrings to be linearly disjoint.

Lemma 4.5. *Let A and B be subrings of a ring C and let $R := A \cap B$. Let R' be a subring of R. Assume that B is a finitely generated projective R'-module. If $A \otimes_{R'} B = A[B]$, then $R' = R$. In particular, A and B are linearly disjoint.*

Proof. For each prime ideal $\mathfrak{p} \subset R'$, the condition $A \otimes_{R'} B = A[B]$ implies that

$$A_{\mathfrak{p}}[B_{\mathfrak{p}}] = (A[B])_{\mathfrak{p}} = (A \otimes_{R'} B)_{\mathfrak{p}} = A_{\mathfrak{p}} \otimes_{R'_{\mathfrak{p}}} B_{\mathfrak{p}}.$$

In addition, note that $R' = R$ if and only if $R'_{\mathfrak{p}} = R_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p} \subset R'$ (see Lemma A.9). Since linearly disjointedness can be checked locally at any prime (Lemma 4.3), we may assume that R' is a local ring. Then B is a finite free R'-module (Proposition 1.7) and we can choose a basis $\{b_i\}_{i \in I}$ for B as R'-module such that $b_0 = 1$ (Corollary A.35).

By hypothesis, $A \otimes_{R'} B = A[B]$, so $\{b_i\}_{i \in I}$ is a basis of $A[B]$ as A-module, via the base change $R' \to A$. Let $r \in R$. As an element in B, it can be expressed as $r = \sum_{i \in I} r'_i b_i$, for some $r'_i \in R'$. Since $r'_0 b_0 = r'_0 \in R$, it follows that $\sum_{i \neq 0} r'_i b_i \in R$. Then we have a linear combination on $\{b_i\}_{i \in I}$, given by

$$\sum_{i \neq 0} r'_i b_i - \left(\sum_{i \neq 0} r'_i b_i \right) \cdot b_0 = 0,$$

with coefficients in R, in particular, in A. Since $\{b_i\}_{i \in I}$ is a basis for $A[B]$ over A, it follows that $r'_i = 0$ for all $i \neq 0$, so $r = r'_0 \in R'$. This proves that $R = R'$ as we wanted. In particular, $A \otimes_R B = A[B]$ and we conclude that A and B are linearly disjoint. □

Finally, we generalize [38, IV, §5, p.162, Lemma], which was established for field extensions, to the setting of rings. It will be very useful in the subsequent sections to prove linear disjointedness by steps.

Lemma 4.6. *Let A and B be subrings of a ring C and let $R := A \cap B$. Let A' be an intermediate subring $R \subseteq A' \subseteq A$. Assume that B is a finite projective R-module. Then A and B are linearly disjoint if and only if A' and B are linearly disjoint, and, also A and $A'[B]$ are linearly disjoint.*

Proof. By Lemma 4.3, we may assume that R is a local ring. Then B is a finite free R-module and we can choose a basis $\{b_i\}_{i \in I}$ that contains the identity element 1 (see Proposition 1.7 and Corollary A.35).

We assume that A and B are linearly disjoint. We have to show that A' and B are linearly disjoint, and also that A and $A'[B]$ are linearly disjoint. We note first that $A' \cap B = R$ and $A' \subseteq A \cap A'[B]$, because $A \cap B = R \subseteq A' \subseteq A$. We have that $\{b_i\}_{i \in I}$ is a basis for B over R by hypothesis. On the one hand, it induces a basis for $A' \otimes_R B$ over A', via the base change $R \to A'$. Since $A' \otimes_R B \to A'[B]$ is a surjective homomorphism, $\{b_i\}_{i \in I}$ generates $A'[B]$ as A'-module. On the other hand, $\{b_i\}_{i \in I}$ is a basis for $A \otimes_R B$, via the base change $R \to A$. Since A and B are linearly disjoint, we have $A \otimes_R B = A[B]$ and $\{b_i\}_{i \in I}$ is indeed a basis for $A[B]$ as A-module (Lemma 4.4).

In particular, $\{b_i\}_{i\in I}$ is an A'-linearly independent subset because $A' \subseteq A$. Thus, as we have proved that $\{b_i\}_{i\in I}$ generates $A'[B]$ as A'-module, we conclude that it is a basis and so A' and B' are linearly disjoint by Lemma 4.4. In addition, $\{b_i\}_{i\in I}$ is a basis for $A \otimes_{A'} A'[B]$ over A via the base change $A' \to A$. Therefore, we have $A \otimes_{A'} A'[B] = A[B]$ and we conclude by Lemma 4.5 that $A' = A \cap A'[B]$ and that A and $A'[B]$ are also linearly disjoint.

Conversely, we suppose that A' and B are linearly disjoint and also that A and $A'[B]$ are linearly disjoint. Since $\{b_i\}_{i\in I}$ is a basis for B over R, and the rings A' and B are linearly disjoint, it follows by Lemma 4.4 that $\{b_i\}_{i\in I}$ is a basis for $A'[B]$ as free A'-module. Moreover, since A and $A'[B]$ are linearly disjoint, it follows again by Lemma 4.4, that $\{b_i\}_{i\in I}$ is also a basis of $A[B]$ as A-module Recall that $\{b_i\}_{i\in I}$ is also a basis for B over R, so A and B are linearly disjoint (Lemma 4.4). □

4.1.2. Generalized p-generating sequences

In this subsection, we restrict the setting to rings of prime characteristic p. We introduce the notion of generalized p-generating sequence for finite extensions of local rings with finite exponent. We begin with notation and properties on some intermediate subrings of a ring extension.

4.7. *Some intermediate subextensions of rings.* Let $A \subseteq C$ be a ring extension. For each integer $e \geq 0$, we denote by $A_e := C^{p^e} \cap A$ the subring of p^e-powers of C that belong to A. Note that the exponent of an element $x \in C$ over A coincides with the minimum integer $e \geq 0$ such that $x^{p^e} \in A_e$ (see Definition 2.1). We have a tower of ring extensions

$$\ldots \subseteq A_{e+1} \subseteq A_e \subseteq \ldots \subseteq A_1 \subseteq A_0 = A.$$

Observe that if $A \subseteq C$ has finite exponent, then $A_e = C^{p^e}$ for all $e \geq \exp(C/A)$. In particular, $\exp(C/A)$ is the minimum integer $e \geq 0$ that satisfies the previous equality of rings. For each $e \geq 0$, we consider the intermediate subextensions of rings

$$A_e \subseteq C^{p^e}.$$

It is clear that C^{p^e} is an A_e-subalgebra of C. In addition, since C can be considered as an A_e-module by restriction of scalars, C^{p^e} is also an A_e-submodule of C. If we assume that C is a finitely generated A-algebra, then C^{p^e} is also finitely generated as an A_e-algebra. In fact, if $C = A[x_1, \ldots, x_n]$, then $C^{p^e} = A_e[x_1^{p^e}, \ldots, x_n^{p^e}]$, because $A^{p^e} \subseteq C^{p^e} \cap A = A_e$.

We note that these intermediate subextensions have a good behaviour under localization at prime ideals.

Lemma 4.8. *Let $A \subseteq C$ be a ring extension of finite exponent. Given an integer $e \geq 0$, let $A_e := C^{p^e} \cap A$ and $\mathfrak{q} \subset A_e$ be a prime ideal. Then there are natural identifications $(C_{\mathfrak{q}})^{p^e} = (C^{p^e})_{\mathfrak{q}}$ and $(C_{\mathfrak{q}})^{p^e} \cap A_{\mathfrak{q}} = (A_e)_{\mathfrak{q}}$.*

Proof. Given an integer $e \geq 0$, we consider the following commutative diagram of ring extensions

$$\begin{array}{ccc} C^{p^e} & \hookrightarrow & C \\ \uparrow & & \uparrow \\ A_e & \hookrightarrow & A \end{array}$$

Note that all the ring extensions in the diagram have finite exponent, since $A \subseteq C$ has finite exponent by assumption. Then the induced maps on the spectra are homeomorphic by Remark 2.2. Given a prime ideal $\mathfrak{q} \subset A_e$, we denote by $\mathfrak{Q} \subset C^{p^e}$ and $\mathfrak{P} \subset C$ the corresponding prime ideals via those homeomorphisms. By Lemma 2.3, we have natural identifications $(C_{\mathfrak{q}})^{p^e} = (C_{\mathfrak{P}})^{p^e}$ and $(C^{p^e})_{\mathfrak{q}} = (C^{p^e})_{\mathfrak{Q}}$. Then any element in $(C_{\mathfrak{q}})^{p^e}$ is of the form x^{p^e}/s^{p^e} with $x \in C$ and $s \in C \setminus \mathfrak{P}$ and any element in $(C^{p^e})_{\mathfrak{q}}$ is of the form x^{p^e}/t with $x \in C$ and $t \in C^{p^e} \setminus \mathfrak{Q}$. Note that $s \in C \setminus \mathfrak{P}$ if and only if $s^{p^e} \in C^{p^e} \setminus \mathfrak{Q}$. Thus, it is clear that $(C_{\mathfrak{q}})^{p^e} = (C^{p^e})_{\mathfrak{q}}$ as we wanted. In addition, we have $(A_e)_{\mathfrak{q}} = (C^{p^e} \cap A)_{\mathfrak{q}} = (C^{p^e})_{\mathfrak{q}} \cap A_{\mathfrak{q}} = (C_{\mathfrak{q}})^{p^e} \cap A_{\mathfrak{q}}$. □

4.9. *Another minimal number of generators.* Let $A \subseteq C$ be a finite extension of local rings with finite exponent. Recall that the A_e-algebras C^{p^e} with $e \geq 0$ are also finite, as we noted in discussion 4.7. For each integer $e \geq 0$, we denote

$$m(e) := \text{minimum number of generators of } C^{p^e} \text{ as } A_e\text{-algebra.}$$

Note that this number coincides with the minimum number of generators of the C^{p^e}-module $\Omega_{C^{p^e}/A}$ by Lemma 2.52. In addition, using the equality $\Omega_{C^{p^e}/A_e} = \Omega_{C^{p^e}/A_e[C^{p^{e+1}}]}$, we see that the number $m(e)$ is also the minimal number of generators for C^{p^e} as $A_e[C^{p^{e+1}}]$-algebra. It is clear that there are inequalities

$$m(0) \geq m(1) \geq m(2) \geq \cdots \geq m(e) \geq m(e+1) \geq \cdots .$$

Moreover, for $e \geq \exp(C/A)$, we have $C^{p^e} = A_e$, so $m(e) = 0$. While, for $0 \leq e < \exp(C/A)$, we have an strict inclusion $A_e \subset C^{p^e}$, so $m(e) > 0$.

We introduce now the notion of generalized p-generating sequence. One may realise that this notion shares many similarities with the notion of generalized normal generating sequence (see Definition 3.2).

Definition 4.10. Let $A \subseteq C$ be a finite extension of local rings with finite exponent. A sequence of elements $x_1, \ldots, x_n \in C$ is a *generalized p-generating sequence* (GpGS) for C over A if $x_1^{p^e}, \ldots, x_{m(e)}^{p^e}$ is a minimal generating set for C^{p^e} as A_e-algebra and $x_i^{p^e} \in A$ for each $i > m(e)$, for all $0 \leq e < \exp(C/A)$.

By convention, the empty set is considered the only GpGS for a trivial extension $A = C$. The results in this section hold immediately for trivial extensions. Hence, in the subsequent proofs we assume the extensions to have positive exponent to avoid trivialities.

Remark 4.11. As it occurs with GNGS, the order of the elements of a GpGS matters. We use the same example as in that case to show this fact (see Remark 3.4). Let A

be a ring and consider the extension $C = A[X,Y]/\langle X^{p^2}, Y^p\rangle$. Let x, y be the classes of X, Y in C. Then $C = A[x,y]$, $C^p = A_1[x^p]$ and $C^{p^2} = A_2$. Thus, x, y is a GpGS whilst y, x is not.

The next lemma shows that there is always a GpGS for a finite extension of local rings with finite exponent.

Lemma 4.12. *Let $A \subseteq C$ be a finite extension of local rings with finite exponent. Then it admits a generalized p-generating sequence.*

Proof. We proceed by induction on $\exp(C/A)$. Let $\{x_1, \dots, x_n\} \subset C$ be any minimal generating set for C as A-algebra. If $\exp(C/A) = 1$, then we have nothing to prove. If $\exp(C/A) > 1$, then $x_1^p, \dots, x_n^p$ generate C^p as A_1-algebra. After rearrangement, we may assume that the first $x_1^p, \dots, x_{m(1)}^p$ form a minimal generating set. Let $R = \{x \in C : x^p \in A\}$. We claim that $R \cup \{x_1, \dots, x_{m(1)}\}$ is a generating set for C as A-algebra. In fact, take any $c \in C$. Then $c^p \in C^p$ and it can be written as an A_1-linear combination of monomials, namely,

$$c^p = \sum_\alpha \Big(a_\alpha (x_1^p)^{\alpha_1} \cdot \ldots \cdot (x_{m(1)}^p)^{\alpha_{m(1)}} \quad \text{for some } a_\alpha \in A_1.$$

Since $a_\alpha \in A_1 = C^p \cap A$, there exists $c_\alpha \in C$ such that $c_\alpha^p = a_\alpha$. In particular, $c_\alpha \in R$. Then the above equality is equivalent to

$$c - \sum_\alpha c_\alpha x_1^{\alpha_1} \cdot \ldots \cdot x_{m(1)}^{\alpha_{m(1)}} \Big)^p = 0.$$

Thus, the element inside the parenthesis and belongs to R. Note that we can write

$$c = \quad c - \sum_\alpha c_\alpha x_1^{\alpha_1} \cdot \ldots \cdot x_{m(1)}^{\alpha_{m(1)}} \Big) + \sum_\alpha \Big(c_\alpha x_1^{\alpha_1} \cdot \ldots \cdot x_{m(1)}^{\alpha_{m(1)}}$$

and this completes the proof of the claim. As a consequence of Nakayama's Lemma (see Proposition A.39), we can find elements $y_1, \dots, y_s \in R$ such that $\{x_1, \dots, x_{m(1)}\} \cup \{y_1, \dots, y_s\}$ is a minimal generating set for C as A-algebra. Since $y_i^p \in A$, it is clear that $x_1, \dots, x_{m(1)}, y_1, \dots, y_s$ is a GpGS for C over A. □

4.13. *Sequence of p-exponents.* Let $A \subseteq C$ be a finite extension of local rings with finite exponent. We set $n := n(0) = m(0)$ for the minimal number of generators for C as A-algebra, as in discussion 4.9. For each $i = 1, \dots, n$ we denote by $f(i)$ the smallest non-negative integer e such that $m(e) < i$. Equivalently, we have

$$m(f(i)) < i \leq m(f(i) - 1). \tag{4.13.1}$$

It is clear that $\exp(C/A) = f(1) \geq f(2) \geq \cdots \geq f(n) \geq 1$. We define $f(1), \dots, f(n)$ to be the *sequence of of p-exponents* of the extension $A \subseteq C$. We observe that the sequence of the minimal number of generators $m(0) \geq m(1) \geq \cdots$ can be recovered from this sequence of p-exponents via the formula

$$m(e) = \max\{i : f(i) > e\}.$$

If $A = C$, then $m(e) = 0$ for all $e \geq 0$ and the sequence of p-exponents is considered to be empty.

Remark 4.14. For a finite extension of local rings $A \subseteq C$ with finite exponent, let $x_1, \ldots, x_n \in C$ be a GpGS, which exists by Lemma 4.12. Note that each p-exponent $f(i)$ is such that $x_i^{p^{f(i)}} \in A$, since $m(f(i)) < i$. Thus, for each $i = 1, \ldots, n$, we have a relation $x_i^{p^{f(i)}} = a_i$ for some $a_i \in A$. Using these relations, we obtain a surjective homomorphism of A-algebras

$$A[X_1, \ldots, X_n] / \left\langle X_i^{p^{f(i)}} - a_i : i = 1, \ldots, n \right\rangle \twoheadrightarrow C\,, \quad X_i \mapsto x_i. \tag{4.14.1}$$

Remark 4.15. In the previous setting, note that the sum of the numbers $f(i)$ from the sequence of p-exponents coincides with the sum of the minimal numbers of generators $m(e)$, i.e.,

$$m(0) + m(1) + \cdots = f(1) + f(2) + \cdots + f(n). \tag{4.15.1}$$

In fact, given $x_1, \ldots, x_n$ a GpGS for C over A, which exists by Lemma 4.12, then for each $0 \leq e \leq \exp(C/A)$, the sequence $x_1^{p^e}, \ldots, x_{m(e)}^{p^e}$ is a GpGS for C^{p^e} over A_e. Note that $m(e)$ counts the number of times that the indexes $m(e-1)+1, \ldots, m(e)$ appear on those GpGS of the intermediate subalgebras and that the index i appears on those GpGS exactly $f(i)$ times.

The next paragraph analyses the connection between generalized p-generating sequences and generalized normal generating sequences.

4.16. *Relation between GpGS and GNGS.* Let $A \subseteq C$ be a finite extension between local rings of finite exponent. Let $m(e)$ be the minimal number of generators for C^{p^e} as A_e-algebra and let $n(e)$ be the minimal number of generators for $C^{[e]}$ as A-algebra (see discussion 3.1). For each $e \geq 0$, there is a natural surjective map

$$A \otimes_{A_e} C^{p^e} \to A[C^{p^e}] =: C^{[e]}.$$

Then it is clear that $m(e) \geq n(e)$ for all $e \geq 0$. In addition, $m(0) = n(0)$. Thus, it is clear that any GpGS contains a GNGS (see Definition 3.2). Moreover, if we have that $m(e) = n(e)$ for $e > 0$, then it follows that any GpGS for C over A is indeed a GNGS. Note also that the map is injective if and only if C^{p^e} and A are linearly disjoint over $A_e = A \cap C^{p^e}$ (see Definition 4.1).

4.1.3. Generalized p-basis

In this subsection, we continue in the setting of rings of prime characteristic p. We review the definition of generalized p-basis and establish some basic properties. We note that this notion was introduced by S. Yuan in [67] to extend the notion of p-basis for extensions of exponent one to the setting of ring extensions of higher exponent.

Definition 4.17. Let $A \subseteq C$ be a ring extension of finite exponent and let $x_1, \ldots, x_n \in C$. For $i = 1, \ldots, n$, denote by e_i the exponent of x_i over A, i.e, the minimal integer $k \geq 0$ such that $x_i^{p^k} \in A$. The collection $\{x_1, \ldots, x_n\}$ is a *generalized p-basis* for C over A if

(i) $x_1, \ldots, x_n$ generate C as A-algebra, i.e, $C = A[x_1, \ldots, x_n]$, and

(ii) $\{x_1, \ldots, x_n\}$ is a *generalized p-independent set* over A, i.e., the set of *generalized reduced monomials* $\{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} : 0 \leq \alpha_i < p^{e_i}\}$ is linearly independent over A.

After rearrangement, we may assume that the exponents are such that $e_1 \geq \cdots \geq e_n$, then $(e_1, \ldots, e_n)$ is the *sequence of exponents* of the generalized p-basis.

Remark 4.18. Let $A \subseteq C$ be a ring extension of finite exponent. Then a collection $\{x_1, \ldots, x_n\} \subset C$ is a generalized p-basis for C over A with sequence of exponents $(e_1, \ldots, e_n)$ if and only if C is a free A-module of rank $p^{e_1+\cdots+e_n}$ with basis given by the set of generalized reduced monomials $\{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} : 0 \leq \alpha_i < p^{e_i}\}$. In other words, if the A-algebra homomorphism $A[X_1, \ldots, X_n] \to C$ which maps X_i to x_i induces an isomorphism

$$A[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}} - x_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} - x_n^{p^{e_n}} \rangle \simeq C.$$

In particular, assuming that $e_1 \geq \ldots \geq e_n$, we have that the exponent of the extension is $\exp(C/A) = e_1$.

Note that if $A \subseteq C$ has exponent at most one, the notion of generalized p-basis coincides with the notion of p-basis (see Definition 2.22). We recall that, by convention, in the trivial case, $A = C$, the empty set is the only (generalized) p-basis, $n = 0$ and the set of reduced monomials is formed by the identity element $\{1_A\}$. Since the concept of generalized p-basis extends the one of p-basis to higher exponent extensions, we will omit the term "generalized" for the p-basis and the reduced monomials when the context is clear.

Remark 4.19. Unlike in the case of exponent at most one, given a field extension of exponent greater than one, it is not true in general that the extension will admit a generalized p-basis (see [62, Example 1.1]). Indeed, the field extensions with this property are called *modular extensions*. We will extend this notion for ring extensions in Section 4.2.

We state in the following lemma some basic and useful properties of generalized p-basis. The proof for this result is straightforward from the definition.

Lemma 4.20. *Let $A \subseteq C$ be a ring extension. Assume that $\{x_1, \ldots, x_n\}$ is a generalized p-basis for C over A with sequence of exponents $\mathbf{e} := (e_1, \ldots, e_n)$. Then*

(1) For each $e \geq 0$, $\{x_1, \ldots, x_n\}$ as a generalized p-basis for C over $C^{[e]}$ with sequence of exponents $\mathbf{e}' := (e_1', \ldots, e_n')$ where $e_i' = \min\{e, e_i\}$.

(2) For any $a_1, \ldots, a_n \in A$, $\{x_1 - a_1, \ldots, x_n - a_n\}$ is also a generalized p-basis for C over A and its sequence of exponents coincides with $\mathbf{e}$.

(3) For any A-algebra A', $\{x_1 \otimes 1, \ldots, x_n \otimes 1\} \subset C \otimes_A A'$ is a generalized p-basis for $C \otimes_A A'$ over A' and its sequence of exponents coincides with $\mathbf{e}$.

We formalize now the notion of *generalized splitting p-basis*. One may note in the next definition that these p-basis induce an special presentation of the ring extension which is the one that appears in the definition of purely inseparable extensions (see Definition 3.11).

Definition 4.21. Let $A \subseteq C$ be a ring extension of finite exponent. A *generalized splitting p-basis* for C over A is a p-basis $\{x_1, \ldots, x_n\}$ such that $x_i^{p^{e_i}} = 0$ for all i. Equivalently, it is a p-basis that induces an A-algebra isomorphism $C \cong A[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$. By convention the empty set is also a splitting p-basis for any trivial extension.

Remark 4.22. We can reformulate the definition of purely inseparable ring extension as follows. A finite ring extension $A \subseteq C$ of finite exponent such that C is projective as A-module is purely inseparable if and only if for each prime ideal $\mathfrak{p} \subset A$, there exists a faithfully flat ring homomorphism $A_{\mathfrak{p}} \to A'$ such that $A' \subseteq C_{\mathfrak{p}} \otimes_A A'$ has a generalized splitting p-basis.

The next proposition shows that a generalized splitting p-basis can always be obtained from an arbitrary generalized p-basis by allowing a suitable base change if necessary. The proof uses the same argument as the one given for the exponent one case (see Proposition 2.27).

Proposition 4.23. *Let $A \subseteq C$ be a ring extension with generalized p-basis $\{x_1, \ldots, x_n\}$ whit sequence of exponents $\mathbf{e} := (e_1, \ldots, e_n)$. Let $A \subseteq A'$ be a ring extension such that, for each $i = 1, \ldots, n$, there exists $y_i \in A'$ with $y_i^{p^{e_i}} = x_i^{p^{e_i}}$. Set $z_i := x_i \otimes 1 - 1 \otimes y_i \in C \otimes_A A'$. Then $\{z_1, \ldots, z_n\}$ is a generalized splitting p-basis for $A' \subset C \otimes_A A'$ with sequence of exponents $\mathbf{e}$.*

Proof. Let $C' := C \otimes_A A'$. By (3) in Lemma 4.20, we have that $\{x_1 \otimes 1, \ldots, x_n \otimes 1\}$ is a generalized p-basis for C' over A'. For each $i = 1, \ldots, n$, we set $z_i := x_i \otimes 1 - 1 \otimes y_i \in C'$. Then, by (2) in Lemma 4.20, $\{z_1, \ldots, z_n\}$ is also a generalized p-basis for C' over A'. Finally, since $x_i^{p^{e_i}} = y_i^{p^{e_i}} \in A$, we have $z_i^{p^{e_i}} = 0 \in C'$, so $\{z_1, \ldots, z_n\}$ is a generalized splitting p-basis for C' over A' with sequence of exponents $\mathbf{e}$. □

Corollary 4.24. *Let $A \subseteq C$ be a ring extension of finite exponent that admits a generalized p-basis of n elements. Then $C \otimes_A C \simeq C[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}} \rangle$ as (left) C-algebras for some $e_i > 0$.*

We focus now on extensions of local rings. We study the behaviour of generalized p-basis for these extensions in relation with some intermediate subextensions. The next lemma implies that any generalized p-basis is in particular a generalized p-generating sequence for extensions of local rings.

Lemma 4.25. *Let $A \subseteq C$ be an extension of local rings. For each $e \geq 0$, let $C^{[e]} := A[C^{p^e}]$. If $\{x_1, \ldots, x_n\}$ is a generalized p-basis for C over A with sequence of exponents $(e_1, \ldots, e_n)$, then $\{x_1^{p^e}, \ldots, x_{m(e)}^{p^e}\}$ is:*

(1) A generalized p-basis for $A_e \subseteq C^{p^e}$. In particular, it is also a p-basis for $A_e[C^{p^{e+1}}] \subseteq C^{p^e}$.

(2) A generalized p-basis for $A \subseteq C^{[e]}$. In particular, it is also a p-basis for $C^{[e+1]} \subseteq C^{[e]}$.

In addition, the sequence $x_1, \ldots, x_n$ is a GpGS, the rings C^{p^e} and A are linearly disjoint and the minimal numbers of generators satisfy $m(e) = n(e) = \max\{i : e_i > e\}$ for all $e \geq 0$.

Proof. We begin with some observations. The sequence of exponents of the generalized p-basis is assumed to be such that $e_1 \geq e_2 \geq \ldots \geq e_n$. For each $e \geq 0$, we define $n_e := \max\{i : e_i > e\}$. Since $C = A[x_1, \ldots, x_n]$, it follows that

$$C^{p^e} = A^{p^e}[x_1^{p^e}, \ldots, x_n^{p^e}] = A_e[x_1^{p^e}, \ldots, x_{n_e}^{p^e}] \quad \text{and} \quad C^{[e]} = A[C^{p^e}] = A[x_1^{p^e}, \ldots, x_{n_e}^{p^e}]$$

because $x_i^{p^e} \in A_e \subseteq A$ for all $e \geq e_i$. Note also that for all $e < e_i$ we have $x_i^{p^e} \notin A$ and, so $x_i^{p^e} \notin A_e$. Since we are in the setting of local rings, any generating set for C^{p^e} as A_e-algebra (respectively for $C^{[e]}$ as A-algebra) contains a minimal generating subset. Hence, we have $n(e) \leq m(e) \leq n_e$. We claim that $n_e = m(e)$. By contradiction, assume that $m(e) < n_e$. Then we can write

$$C^{p^e} = A_e[x_{\lambda_1}^{p^e}, \ldots, x_{\lambda_{m(e)}}^{p(e)}] \quad \text{for some } \lambda_i \in \{1, \ldots, n_e\}$$

and there exists $k \neq \lambda_i$ for all $i = 1, \ldots, m(e)$, such that $x_k^{p^e} \notin A_e$ and $x_k^{p^e} \in A_e[x_{\lambda_1}^{p^e}, \ldots, x_{\lambda_{m(e)}}^{p(e)}]$. This implies the existence of a non-trivial relation of the generalized reduced monomials, which is a contradiction because $\{x_1, \ldots, x_n\}$ is a generalized p-basis. Therefore, $m(e) = n_e$.

We prove (1) and (2) simultaneously. The above discussion implies that

$$C^{p^e} = A_e[x_1^{p^e}, \ldots, x_{m(e)}^{p^e}] \quad \text{and} \quad C^{[e]} = A[x_1^{p^e}, \ldots, x_{m(e)}^{p^e}].$$

In particular, since $m(e) = n_e$, we have $x_i^{p^e} \in A$ for all $i > m(e)$. Thus, $x_1, \ldots, x_n$ is a GpGS. It is clear that $x_i^{p^e}$ has exponent $e_i - e$ over A_e and over A. Note that

$$\{(x_1^{p^e})^{\alpha_1} \cdot \ldots \cdot (x_{m(e)}^{p^e})^{\alpha_{m(e)}} : 0 \leq \alpha_i < p^{e_i - e}\}$$

is a subset of the generalized reduced monomials associated to the generalized p-basis $\{x_1, \ldots, x_n\}$. Thus, it is linearly independent over A and, in particular, over A_e. Therefore, $\{x_1^{p^e}, \ldots, x_{m(e)}^{p^e}\}$ is a generalized p-basis for both the extension $A_e \subseteq C^{p^e}$ and $A \subseteq C^{[e]}$. It follows immediately that it is also a p-basis for the extensions $A_e[C^{p^{e+1}}] \subseteq C^{p^e}$ and $C^{[e+1]} \subseteq C^{[e]}$.

Finally, the discussion in the previous paragraph implies that C^{p^e} is a free A_e-module and $C^{[e]}$ is a free A-module with the same basis. Then, by Lemma 4.4, the rings C^{p^e} and A are linearly disjoint and so the map $C^{p^e} \otimes_{A_e} A \to C^{[e]}$ is an isomorphism of finite free A-modules. Hence, the ranks coincide and we conclude that $m(e) = n(e)$. □

The following lemma exhibits a method to obtain a generalized p-basis for a finite exponent extension of local rings by steps related to some intermediate extensions.

Lemma 4.26. *Let $A \subseteq C$ be a finite exponent extension of local rings and let $\{x_1, \dots, x_n\} \subset C$. Fix an integer $e \geq 0$ and denote $C^{[e]} := A[C^{p^e}]$ and $n_e := \max\{i : e_i > e\}$. If the following conditions hold:*

(1) the set $\{x_1, \dots, x_n\}$ is a generalized p-basis for $C^{[e]} \subseteq C$, and

(2) the set $\{x_1^{p^e}, \dots, x_{n_e}^{p^e}\}$ is a generalized p-basis for $A \subseteq C^{[e]}$.

Then $\{x_1, \dots, x_n\}$ is a generalized p-basis for $A \subseteq C$. In particular, $n_e = n(e)$, the minimal number of generators for $C^{[e]}$ as A-algebra.

Proof. Let e_i be the exponent of x_i over A and let e_i' be the exponent over $C^{[e]}$. Note that $e_i' = e$ for $i \leq n_e$, and $e_i' = e_i$ for $i > n_e$. That is, $e_i' = \min\{e, e_i\}$ for $i = 1, \dots, n$. Then the set of generalized reduced monomials associated to $\{x_1, \dots, x_n\}$ can be expressed as the following disjoint union of sets

$$\{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} : 0 \leq \alpha_i < p^{e_i}\} = \{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} : 0 \leq \alpha_i < p^{e_i'}\} \bigcup \left(\{x_1^{p^e \alpha_1} \cdot \ldots \cdot x_{n_e}^{p^e \alpha_{n_e}} : 0 \leq \alpha_i < p^{e_i - e}\} \right.$$

Observe that the first subset above is a basis for C as $A[C^{p^e}]$-module and that the second subset above is a basis for $A[C^{p^e}]$ as A-module, respectively by (1) and (2) in the statement. Thus, the disjoint union of the subsets forms a basis for C as A-module. By Remark 4.18, this implies that $\{x_1, \dots, x_n\}$ is a generalized p-basis for C over A with sequence of exponents $(e_1, \dots, e_n)$. In addition, we conclude that $n(e) = m(e) = n_e$ by Lemma 4.25. □

As a direct consequence of the two previous lemmas, we obtain a criteria for a collection of elements to be a generalized p-basis for a finite exponent extension of local rings.

Corollary 4.27. *Let $A \subseteq C$ be a finite exponent extension between local rings. A collection of elements $\{x_1, \dots, x_n\}$ is a generalized p-basis for $A \subseteq C$ if and only if $\{x_1^{p^e}, \dots, x_{n(e)}^{p^e}\}$ is a p-basis for $C^{[e+1]} \subseteq C^{[e]}$ for each $0 \leq e < \exp(C/A)$.*

4.2. On modular extensions of rings

In this section, all the rings have prime characteristic p. In Subsection 4.2.1, we use generalized p-basis to give a modular extensions of rings that extends the classical one for field extensions. In Subsection 4.2.2, we deepen in the relation of modular extensions and linearly disjointedness to show that these extensions are a particular class of purely inseparable extensions that satisfy some conditions of linearly disjointedness.

4.2.1. Basics on modular extensions

We introduce now a notion of modular extension for rings in general and we establish some basic properties that are easily deduced from it. We note that our definition of modular ring extension extends the original definition of modular extension of fields given by the equivalents conditions of [62, Theorem 1] from M.S. Sweedler.

Definition 4.28. A finite extension of rings $A \subseteq C$ is a *modular extension* if the following conditions hold

(1) $A \subseteq C$ has finite exponent;

(2) C is a projective A-module; and

(3) for each prime ideal $\mathfrak{p} \subset A$, the extension $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}}$ has a generalized p-basis.

Note that a modular extension of exponent at most one is exactly a Galois extension (see Definition 2.41). In particular, any trivial extension, $A = C$, is considered to be a modular extension of exponent zero. Thus, the notion of modular extension and purely inseparable extensions coincide for ring extensions of exponent at most one. However, this notions are not the same for the higher exponent case (see Remark 4.19)

Remark 4.29. Any ring extension $A \subseteq C$ that admits a generalized p-basis is a modular extension. In fact, C is a free A-module of finite rank as we noted in Remark 4.18. In particular, C is projective as A-module. Since $A \subseteq C$ has a generalized p-basis, for every prime ideal $\mathfrak{p} \subset A$, the extension $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}} := C \otimes_A A_{\mathfrak{p}}$ obtained by the base change $A \to A_{\mathfrak{p}}$ also admits a p-basis by Lemma 4.20.(3).

Remark 4.30. Note that condition (iii) in the above definition already implies that $C_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module for all prime ideal $\mathfrak{p} \subset A$ (see Remark 4.18). Then, by Proposition 1.7, condition (ii) in the definition of modular extension can be replaced by the condition that C is an A-module of finite presentation.

Remark 4.31. Observe that condition (iii) in the definition of modular extension only needs to be verified at maximal ideals. In fact, assume that $A_{\mathfrak{m}} \subseteq C_{\mathfrak{m}}$ admits a generalized p-basis for any maximal ideal $\mathfrak{m} \subset A$. Given a prime ideal $\mathfrak{p} \subset A$, there is a maximal ideal such that $\mathfrak{p} \subseteq \mathfrak{m}$. The extension $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}}$ coincides with the base change of $A_{\mathfrak{m}} \subseteq C_{\mathfrak{m}}$ via the localization map $A_{\mathfrak{m}} \to A_{\mathfrak{p}}$. Thus, $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}}$ has a generalized p-basis by Lemma 4.20.(3).

The next lemma shows that modular extensions behave well under base extension as a consequence of Lemma 4.20. The proof is similar to the one given to prove the good behaviour of Galois extensions of exponent one with base change (see Proposition 2.45.(2))

Lemma 4.32. *Let $A \subseteq C$ be a modular extension. Then for any homomorphism of rings $A \to A'$, the extension $A' \subseteq C \otimes_A A'$ is modular.*

Proof. Let $C' := C \otimes_A A'$. Since $A \subseteq C$ is a finite projective ring extension, we have that $A' \subseteq C'$ is also a finite extension such that C' is projective as A'-module

by Remark 1.16. In addition, the extension $A' \subseteq C'$ has finite exponent by Lemma 2.8. Thus, to show that $A' \subseteq C'$ is modular it only lefts to show that for any prime ideal $\mathfrak{q} \subset A'$, the extension $A'_{\mathfrak{q}} \subseteq C'_{\mathfrak{q}}$ has a generalized p-basis. Recall that there is a morphism $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$ induced by $A \to A'$. Given a prime ideal $\mathfrak{q} \subset A'$, let $\mathfrak{p} \subset A$ be the prime ideal such that $\mathfrak{q} \mapsto \mathfrak{p}$ via the previous morphism. Hence, we have natural maps $A_{\mathfrak{p}} \to A_{\mathfrak{p}} \otimes_A A' \to A'_{\mathfrak{q}}$. Then, by Lemma 4.20.(3), the generalized p-basis for $C_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$ induces a generalized p-basis for $C'_{\mathfrak{q}}$ over $A'_{\mathfrak{q}}$ as we wanted. □

We demonstrate that modular extensions of rings are a subclass of purely inseparable extensions of rings.

Proposition 4.33. *Let $A \subseteq C$ be a modular extensions of rings. Then $A \subseteq C$ is purely inseparable.*

Proof. By definition, since the extension is modular, $A \subseteq C$ is a finite ring extension of finite exponent such that C is a projective A-module. Thus, to show that it is purely inseparable it only lefts to show that for each prime ideal $\mathfrak{p} \subset A$ there exists a faithfully flat map $A_{\mathfrak{p}} \to A'$ such that $A' \subseteq C_{\mathfrak{p}} \otimes A'$ has a generalized splitting p-basis (see Definition 3.11). By assumption, the extension $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}}$ has a generalized p-basis. In addition, $A_p \to C_{\mathfrak{p}}$ is faithfully flat (see Remark 1.16). Then we conclude that $C_{\mathfrak{p}} \subseteq C_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} C_{\mathfrak{p}}$ has a generalized splitting p-basis by Corollary 4.24. □

As a direct consequence of the properties of generalized p-basis from Subsection 4.1.3, we obtain the following result for the intermediate subalgebras of a modular extension $A \subseteq C$. We will see that the converse is true under the assumption that C^{p^e} and A are linearly disjoint (Proposition 4.37).

Lemma 4.34. *Let $A \subseteq C$ be a modular extension. For each integer $e \geq 0$, denote $C^{[e]} := A[C^{p^e}]$. Then $A \subseteq C^{[e]}$ and $C^{[e]} \subseteq C$ are modular for all $e \geq 0$.*

Proof. It is clear that $A \subseteq C^{[e]}$ and $C^{[e]} \subseteq C$ are finite extensions of finite exponent. Moreover, by Proposition 4.33, we know that $A \subseteq C$ is purely inseparable. In particular, $A \subseteq C$ is an $\mathcal{F}$-extension by Theorem 3.25. So C is a projective $C^{[e]}$-module and $C^{[e]}$ is a projective A-module by Remark 3.22 and Lemma 3.24. Finally, since localization at prime ideals behaves well with the Frobenius endomorphism (see Lemma 4.8 and 2.3), we conclude by Lemma 4.20.(1) and Lemma 4.25.(2) that $A \subseteq C^{[e]}$ and $C^{[e]} \subseteq C$ are modular. □

4.2.2. Modular extensions and linearly disjointedness

In this subsection, we study the relation between modular extensions and linearly disjointedness. On the one hand, we show that, for any modular extension $A \subseteq C$, the subrings C^{p^e} and A are linearly disjoint for all $e \geq 0$. On the other hand, we prove that a purely ring inseparable extension satisfying these condition is modular. In conclusion, this implies that a modular extension is exactly a purely inseparable extension satisfying the mentioned condition. Using this characterization we re-obtain some interesting results of modular and purely inseparable field extensions.

Proposition 4.35. *Let $A \subseteq C$ be a modular extension. Then C^{p^e} and A are linearly disjoint for all $e \geq 0$.*

Proof. By Lemma 4.3 and Lemma 4.8, we know that C^{p^e} and A are linearly disjoint if and only if $(C_{\mathfrak{q}})^{p^e}$ and $A_{\mathfrak{q}}$ are linearly disjoint for every prime ideal $\mathfrak{q} \subset A_e$. Denote by $\mathfrak{p}$ the prime ideal in A corresponding to the prime ideal $\mathfrak{q}$ via the homeomorphism induced by $A_e \to A$ (see Remark 2.2). By Lemma 2.3, we have that $(C_{\mathfrak{q}})^{p^e} = (C_{\mathfrak{p}})^{p^e}$ and $A_{\mathfrak{q}} = A_{\mathfrak{p}}$. Since $A \subseteq C$ is modular, the extension $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}}$ has a generalized p-basis for every prime ideal $\mathfrak{p} \subset A$. Thus, $(C_{\mathfrak{p}})^{p^e}$ and $A_{\mathfrak{p}}$ are linearly disjoint by Lemma 4.25 and this completes the proof. □

We have already proved that modular ring extensions are a subclass of purely inseparable extensions. We will show now that they are indeed the subclass of purely inseparable extensions $A \subseteq C$ such that C^{p^e} and A are linearly disjoint for each $e \geq 0$. The proof will involve the following proposition on purely inseparable extensions of local rings.

Proposition 4.36. *Let $A \subseteq C$ be a purely inseparable extension of local rings. If the numbers of minimal generators are such that $m(e) = n(e)$ for all $e \geq 0$, then $A \subseteq C$ is modular.*

Proof. Let $x_1, \ldots, x_n$ be a generalized p-generating sequence for C over A, which exists by Lemma 4.12. Since $m(e) = n(e)$ for all $e \geq 0$, the sequence $x_1, \ldots, x_n$ is a generalized normal generating sequence (GNGS) as we noted in discussion 4.16. In addition, the p-exponents and the normal exponents coincide, that is, $f(i) = e(i)$ for all $i = 1, \ldots, n$ (see discussions 3.6 and 4.13). Thus, the relations of the elements of the GNGS are $x_i^{p^{e(i)}} = a_i$ for some $a_i \in A$ (see Remark 3.7). Since $A \subseteq C$ is purely inseparable, it is also a normal generating sequence (NGS) and we have an isomorphism

$$A[X_1, \ldots, X_n] / \left\langle X_i^{p^{e(i)}} - a_i : i = 1, \ldots, n \right\rangle \xrightarrow{\sim} C\,, \quad X_i \mapsto x_i. \tag{4.36.1}$$

by Proposition 3.10. Then $x_1, \ldots, x_n$ is a generalized p-basis for C over A by Remark 4.18. Finally, we conclude that $A \subseteq C$ is modular as we noted in Remark 4.29. □

Proposition 4.37. *Let $A \subseteq C$ be a purely inseparable extension of rings. If C^{p^e} and A are linearly disjoint for all $e \geq 0$, then $A \subseteq C$ is modular.*

Proof. By definition, since the extension is purely inseparable, $A \subseteq C$ is a finite ring extension of finite exponent such that C is a projective A-module. Thus, to show that it is modular it only lefts to show that for each prime ideal $\mathfrak{p} \subset A$, the extension $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}}$ is modular. By assumption, the extension $A_{\mathfrak{p}} \subseteq C_{\mathfrak{p}}$ is a purely inseparable of local rings. We prove that the minimal numbers of generators for this extension are such that $m(e) = n(e)$ for all $e \geq 0$ to apply Proposition 4.36. This follows if we show that $(C_{\mathfrak{p}})^{p^e}$ and $A_{\mathfrak{p}}$ are linearly disjoint for all $e \geq 0$ (see Remark 4.16), so we prove this condition. Given a prime ideal $\mathfrak{p} \subset A$, we denote by $\mathfrak{q}$ the prime ideal in A_e corresponding to the prime $\mathfrak{p}$ via the homeomorphism induced by $A_e \to A$ (see

Remark 2.2). By Lemma 2.3 and Lemma 4.8, we have that $(C_{\mathfrak{p}})^{p^e} = (C_{\mathfrak{q}})^{p^e} = (C^{p^e})_{\mathfrak{q}}$ and $A_{\mathfrak{p}} = A_{\mathfrak{q}}$. Since C^{p^e} and A are linearly independent, we have that $(C_{\mathfrak{q}})^{p^e}$ and $A_{\mathfrak{q}}$ are linearly disjoint by Lemma 4.3 and this completes the proof. □

If we combine Proposition 4.33 and Proposition 4.37, we obtain the following characterization for modular extensions of rings in terms of linearly disjointedness.

Theorem 4.38. *Let $A \subseteq C$ be a finite ring extension of finite exponent. Then $A \subseteq C$ is modular if and only if the following conditions hold:*

(1) C^{p^e} and A are linearly disjoint for all $e \geq 0$; and

(2) $A \subseteq C$ is purely inseparable.

As an immediate consequence, we see that linearly disjointedness allows us to define modular extensions inductively, using the intermediate subalgebras $C^{[e]} := A[C^{p^e}]$.

Corollary 4.39. *Let $A \subseteq C$ be a finite ring extension of finite exponent. Then $A \subseteq C$ is modular if and only if C^{p^e} and A are linearly disjoint, and there exists $k \geq 0$ such that $A \subseteq C^{[k]}$ and $C^{[k]} \subseteq C$ are modular.*

Proof. If $A \subseteq C$ is modular, then the conditions hold by Proposition 4.35 and Lemma 4.34. Conversely, assume that C^{p^e} and A are linearly disjoint, and that $A \subseteq C^{[k]}$ and $C^{[k]} \subseteq C$ are modular for an integer $k \geq 0$. By Theorem 4.38, these extensions are purely inseparable. In particular, $C^{[e+1]} \subseteq C^{[e]}$ are Galois for all $e \geq 0$ by Theorem 3.18. Thus, $A \subseteq C$ is purely inseparable. Using that C^{p^e} and A are linearly disjoint, the conclusion follows by Theorem 4.38 □

Furthermore, using the above characterization of modular extensions (Theorem 4.38) and the characterization of purely inseparable extensions as flat families (Theorem 3.25), we easily obtain the next characterization involving the modularity of the fibers.

Theorem 4.40. *Let $A \subseteq C$ be a finite extension of finite exponent. Then $A \subseteq C$ is modular if and only if the following condition holds:*

(1) $A \subseteq C$ is an $\mathcal{F}$-extension;

(2) C^{p^e} and A are linearly disjoint for all $e \geq 0$; and

(3) For each maximal ideal $\mathfrak{m} \subset A$, the extension $A/\mathfrak{m} \subseteq C/\mathfrak{m}C$ is modular.

Moreover, condition (3) can be replaced by

(3') For each maximal ideal $\mathfrak{m} \subset A$, the extension $A/\mathfrak{m} \subseteq C/\mathfrak{m}C$ is purely inseparable.

Proof. If $A \subseteq C$ is modular, then $A \subseteq C$ is purely inseparable by Proposition 4.33. In particular, $A \subseteq C$ is and $\mathcal{F}$-extension by Theorem 3.25. In addition, C^{p^e} and A are linearly disjoint by Proposition 4.35. Finally, given a maximal ideal $\mathfrak{m} \subset A$, the extension $A/\mathfrak{m} \subseteq C/\mathfrak{m}C$, obtained via the base change $A \to A/\mathfrak{m}$, is also modular by Lemma 4.32. In particular, it is purely inseparable.

Conversely, we assume that $A \subseteq C$ satisfies conditions (1), (2) and (3'), since (3) already implies (3') by Proposition 4.33. Note that (1) and (3') imply that $A \subseteq C$ is purely inseparable by Theorem 3.25. Finally, we conclude that $A \subseteq C$ is a modular extension because any purely inseparable extension satisfying (2) is modular by Proposition 4.37. □

Finally, as a consequence of the above characterizations of modular ring extensions, we re-obtain some well-known results of finite field extensions. On the one hand, we deduce a characterization for modular field extensions, which was originally established by M. E. Sweedler.

Corollary 4.41 ([62, Theorem 1])**.** *Let $K \subseteq L$ be a finite purely inseparable extension of fields. Then $K \subseteq L$ is modular if and only if L^{p^e} and K are linearly disjoint for all $e \geq 0$.*

On the other hand, we show that purely inseparable finite field extensions can be characterized by the modularity of the induced extension at any algebraic closure.

Proposition 4.42. *Let $K \subseteq L$ be a finite field extension and let $\bar{K}$ be an algebraic closure of K. Then $K \subseteq L$ is purely inseparable if and only if $\bar{K} \subseteq L \otimes_K \bar{K}$ is modular.*

Proof. We assume first that $K \subseteq L$ is purely inseparable and proceed by induction on $\exp(L/K)$. If $\exp(L/K) \leq 1$, then $K \subseteq L$ is Galois and in particular, it is modular. By Lemma 4.32, we deduce that the extension $\bar{K} \subseteq L \otimes_K \bar{K}$, obtained via the base change $K \to \bar{K}$, is also modular. We suppose now that $\exp(L/K) > 1$. Then the extension $\bar{K} \subseteq L' := L \otimes_K \bar{K}$ is purely inseparable by Proposition 3.20.(1). In addition, we have $\exp(L'/\bar{K}) \leq \exp(L/K)$ by Lemma 2.8. In particular, $\bar{K} \subseteq \bar{K}[L'^p]$ is also purely inseparable and has exponent $\exp(L'/\bar{K}) - 1 < \exp(L/K)$. Then we can apply the inductive hypothesis to deduce that $\bar{K} \subseteq \bar{K}[L'^p]$ is modular. Note that $\bar{K} \subseteq L'^p$ because $\bar{K} = \bar{K}^p$ as $\bar{K}$ is algebraically closed. Therefore, $\bar{K} \subseteq L'^p$ is modular. By Proposition 4.35, L'^{p^e} and $\bar{K}$ are linearly disjoint for all $e > 0$. Note that L' and $\bar{K}$ are clearly linearly disjoint, since $\bar{K} \subseteq L'$. Thus, L'^{p^e} and $\bar{K}$ are linearly disjoint for all $e \geq 0$. By Corollary 4.41, we conclude that $\bar{K} \subseteq L' = L \otimes_K \bar{K}$ is modular.

Conversely, we assume that $\bar{K} \subseteq L \otimes_K \bar{K}$ is modular. In particular, it has finite exponent. Since $K \to \bar{K}$ is a faithfully flat homomorphism, the extension $K \subseteq L$ also has finite exponent by Lemma 2.9. Thus, $K \subseteq L$ is purely inseparable. □

APPENDIX A
Commutative algebra

In this appendix, we collect some classical definitions, basic properties and well-known results that are used throughout this thesis. In what follows, all rings are assumed to be commutative with identity and all ring homomorphisms are supposed to send the identity element of the source ring into the identity element of the target ring, unless otherwise stated.

A.1. Some concepts of rings

In this subsection, we recall some concepts related to Noetherian, Artinian and complete intersection rings.

On Noetherian and Artinian rings.

A.1. *Noetherian and Artinian rings.* A ring R is

- *Noetherian* if any ascending chain of ideals $I_0 \subseteq I_1 \subseteq \dots$ becomes stationary, i.e., there exists an integer n such that $I_i = I_n$ for all $i \geq n$.
- *Artinian* if any descending chain of ideals $I_0 \supseteq I_1 \supseteq \dots$ becomes stationary.

Note that any field is Noetherian and Artinian. Moreover, we know that every Artinian ring is also Noetherian (see [47, Theorem 3.2]).

Proposition A.2 ([2, Proposition 6.2]). *Let R be a ring. The following conditions are equivalent:*

(1) R is Noetherian.

(2) Every ideal of R is finitely generated.

Proposition A.3 ([2, Proposition 6.6]). *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. Then the quotient ring R/I is Noetherian.*

Proposition A.4 ([2, Proposition 6.10]). *Let $K \to R$ be an homomorphism of rings where K is a field. If R has finite dimension as K-vector space, then R is an Artinian ring. In particular, R is Noetherian.*

Proposition A.5 ([2, Corollary 6.11]). *Let $(R, \mathfrak{m})$ be a local ring such that its maximal ideal is nilpotent. Then R is Artinian if and only if it is Noetherian.*

A.6. *Embedding dimension.* Let $(R, \mathfrak{m})$ be a Noetherian local ring. The *embedding dimension* of R is the minimal number of generators for $\mathfrak{m}$. We denote it by $\mathrm{embdim}(R)$. By Nakayama's Lemma (Corollary A.35), the embedding dimension of R coincides with the minimal number of generators of $\mathfrak{m}/\mathfrak{m}^2$ as $R/\mathfrak{m}$-vector space.

On complete intersection rings

A.7. *Completion.* Let R be a ring and let $I \subseteq R$ be an ideal.

- A *descending filtration of ideals* of R is a sequence of ideals $R = I_0 \supseteq I_1 \supseteq \dots$ that we denote by $\{I_k\}_{k\in\mathbb{N}}$.
- The *completion* of R with respect to a descending filtration $\{I_k\}_{k\in\mathbb{N}}$ is the ring $\hat{R} := \varprojlim R/I_k$, where the transition morphisms between R/I_k are reduction modulo I_k.
- R is *complete* with respect to I if there is an isomorphism $R \xrightarrow{\sim} \hat{R}$, where $\hat{R}$ is the completion with respect to the *I-adic filtration* $\{I_k\}_{k\in\mathbb{N}}$ defined by $I_k := I^k$.

A.8. *Complete intersection rings.* Let $(R, \mathfrak{m})$ be a Noetherian local ring and $\hat{R}$ be the completion of R with respect to the $\mathfrak{m}$-adic filtration. By the Cohen Structure Theorem ([47, 10, §29]), we can write $\hat{R} = S/I$ for a regular Noetherian complete local ring S. The ring R is a *complete intersection* if the minimal number of generators of I coincides with $\dim(S) - \dim(R)$, where here dim denotes the Krull dimension of the ring.

A.2. Some properties of modules

In this subsection, we collect some basic definitions and properties about modules over a ring.

On exact sequences

Lemma A.9 ([9, II, §3.3, Theorem 1]). *Let $K \to M \to N$ be a sequence of R-modules. Then the following assertions are equivalent:*

(1) The sequence $K \to M \to N$ is exact.

(2) For every prime ideal $\mathfrak{p} \subset R$, the sequence $K_\mathfrak{p} \to M_\mathfrak{p} \to N_\mathfrak{p}$ is exact.

(3) For every maximal ideal $\mathfrak{m} \subset R$, the sequence $K_\mathfrak{m} \to M_\mathfrak{m} \to N_\mathfrak{m}$ is exact.

Lemma A.10 (Splitting Lemma, [8, §1.5, p.39]). *Let $0 \to K \xrightarrow{u} M \xrightarrow{v} N \to 0$ be a short exact sequence of R-modules. Then the following statements are equivalent:*

(1) The sequence is left split, i.e., there exists a morphism $u' \colon M \to K$ such that $u' \circ u = \mathrm{id}_K$.

(2) The sequence is right split, i.e., there exists a morphism $v' \colon N \to M$ such that $v \circ v' = \mathrm{id}_N$.

(3) The sequence is split exact, i.e., it is isomorphic to the exact sequence $0 \to K \to K \oplus N \to N \to 0$.

In (1), we say that u' is a retraction for u. In (2), we say that v' is a section for v.

On flat and faithfully flat modules

A.11. *Flat and faithfully flat modules.* An R-module M is

- *Flat* if for every injective map of R-modules $N' \to N$, the map $N' \otimes_R M \to N \otimes_R M$ obtained by tensoring with M over R is also injective.
- *Faithfully flat* if M is flat and for every R-module N the equality $M \otimes_R N = 0$ implies $N = 0$.

We collect some useful characterizations of flat and faithfully flat modules over a ring.

Proposition A.12 ([9, I, §2.3, Proposition 1 and Proposition 4]). *Let M be an R-module. The following conditions are equivalent:*

(1) M is flat.

(2) For every short exact sequence $0 \to N' \to N \to N'' \to 0$ of R-modules, the tensored sequence $0 \to N' \otimes_R M \to N \otimes_R M \to N'' \otimes_R M \to 0$ is exact.

(3) For every exact sequence $N' \to N \to N''$ of R-modules, the tensored sequence $N' \otimes_R M \to N \otimes_R M \to N'' \otimes_R M$ is exact.

(4) For every exact sequence $0 \to K \to N \to M \to 0$ of R-modules and for every R-module M', the tensored sequence $0 \to K \otimes_R M' \to N \otimes_R M' \to M \otimes_R M' \to 0$ is exact.

(5) For every finitely generated ideal $I \subseteq R$, the homomorphism $I \otimes_R M \to M, x \otimes m \mapsto xm$ is injective.

Proposition A.13 ([9, II, §3.4, Proposition 1.5]). *Let M be an R-module. Then M is flat if and only if $M_\mathfrak{p}$ is flat as $R_\mathfrak{p}$-module for every prime ideal $\mathfrak{p} \subset A$.*

Proposition A.14 ([8, §4.2, Proposition 11]). *Let M be an R-module. The following conditions are equivalent:*

(1) M is faithfully flat.

(2) A sequence of R-modules $N' \to N \to N''$ is exact if and only if the sequence obtained by tensoring with M over R, i.e., $M \otimes_R N' \to M \otimes_R N \to M \otimes_R N''$, is exact.

(3) M is flat and given a morphism of R-modules $\varphi\colon N' \to N$ such that $\varphi \otimes_R \mathrm{id}_M\colon N' \otimes_R M \to N \otimes_R M$ is the zero morphism, then $\varphi = 0$.

(4) M is flat and for every maximal ideal $\mathfrak{m} \subset R$, we have $\mathfrak{m}M \neq M$.

We recall that being flat behaves well under base change and faithfully flat descent.

Proposition A.15 ([8, §4.4, Proposition 1])**.** *Let $R \to S$ be an homomorphism of rings and let M be an R-module.*

(1) If M is flat, then $M \otimes_R S$ is a flat S-module.

(2) If $R \to S$ is faithfully flat and $M \otimes_R S$ is a flat S-module, then M is flat as R-module.

The property of being faithfully flat also behaves well by base change.

Proposition A.16 ([9, I, §3.4, Proposition 5])**.** *Let $R \to R'$ be an homomorphism of rings and let M be an R-module. If M is faithfully flat R-module, then the R'-module $M \otimes_R R'$ is also faithfully flat.*

The following proposition relates being flat and faithfully flat with restriction of scalars.

Proposition A.17 ([9, I, §2.7, Corollary 3 and §3.4, Proposition 7])**.** *Let $R \to S$ be an homomorphism of rings such that S is (faithfully) flat as R-module. If M is a (faithfully) flat S-module, then the R-module M obtained by restriction of scalars is (faithfully) flat.*

We include some useful characterizations of faithfully flat homomorphisms of rings.

Proposition A.18 ([9, I, §3.5, Proposition 9, (a)⇔(b)])**.** *Let $R \to S$ be an homomorphism of rings. Then $R \to S$ is faithfully flat if and only if $R \to S$ is injective and the quotient R/S is a flat R-module.*

Proposition A.19 ([9, I, §3.5, Proposition 9, (a)⇔(e)])**.** *Let $R \to S$ be a flat homomorphism of rings. Then $R \to S$ is faithfully flat if and only if the induced map on the spectra $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective.*

As a consequence of the above results we obtain the following property for flat local morphisms of rings.

Corollary A.20. *Let $(R, \mathfrak{m}_R) \to (S, \mathfrak{m}_S)$ be a flat local homomorphism of local rings. Then the map is faithfully flat and injective.*

Proof. We have $S \otimes_R (R/\mathfrak{m}_R) = S/\mathfrak{m}_R S \neq 0$, since $\mathfrak{m}_R S$ is contained in $\mathfrak{m}_S$. Then by Proposition A.14, $R \to S$ is faithfully flat, and, by Proposition A.18, it is also injective. □

On the annihilator of an element

A.21. *Annihilator ideal.* Let M be an R-module. Given $m \in M$, the *annihilator of* m is the ideal

$$\operatorname{ann}_R(m) := \{x \in R : xm = 0\}.$$

Lemma A.22. *Let $R \to S$ be a flat homomorphism of rings. Let M be an R module and $m \in M$. Then* $\operatorname{ann}_R(m)S = \operatorname{ann}_S(m \otimes 1)$.

Proof. We have a left exact sequence $0 \to \operatorname{ann}_R(m) \to R \to M$ of R-modules where the map $R \to M$ is defined by $x \to xm$. Since $R \to S$ is flat, the induced sequence $0 \to \operatorname{ann}_R(m) \otimes_R S \to S \to M \otimes_R S$ is also left exact. Since $\operatorname{ann}_R(m) \otimes_R S = \operatorname{ann}_R(m)S$ and the map $S \to M \otimes_R S$ is given by $s \to s(m \otimes 1)$, we conclude that $\operatorname{ann}_R(m)S = \operatorname{ann}_S(m \otimes 1)$. □

On finitely generated and finitely presented modules

A.23. *Finiteness conditions.* Let M be an R-module.

- M is *finitely generated* (or *finite*) if there exists a surjection $R^n \to M$ for some positive integer n.
- M is *of finite presentation* if there exists a right exact sequence $R^m \to R^n \to M \to 0$ for some positive integers m, n.

In particular, every module of finite presentation is finitely generated. If R is a Noetherian ring, then the converse is true and these finiteness conditions coincide (see [9, I, §8, Lemma 8]).

The finiteness conditions defined above can be checked locally at an open covering.

Lemma A.24 ([9, II, §5.1, Corollary of Proposition 3])**.** *Let $f_1, \ldots, f_r \in R$ be elements that generate the unit ideal and let M be an R-module. Then M is finitely generated (resp. of finite presentation) if and only if M_{f_i} is finitely generated (resp. of finite presentation) as R_{f_i}-module for all $i = 1, \ldots, r$.*

Proposition A.25 ([8, §1.5, Proposition 5 and Proposition 6], [47, 1 §2, Ex. 2.5])**.** *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules.*

(1) If M' and M'' are finitely generated (resp. of finite presentation), then M is also finitely generated (resp. of finite presentation).

(2) If M is finitely generated, then M'' is finitely generated.

(3) If M is finitely generated and M'' is of finite presentation, then M' is finitely generated.

(4) If M is of finite presentation and M' is finitely generated, then M'' is of finite presentation.

Being finitely generated and finitely presented behaves by base change of rings and faithfully flat descent.

Proposition A.26 ([8, §4.4, Proposition 1])**.** *Let $R \to S$ be an homomorphism of rings. Let M be an R-module.*

(1) If M is finitely generated (resp. of finite presentation), then $M \otimes_R S$ is also finitely generated (resp. of finite presentation) as S-module.

(2) If $R \to S$ is faithfully flat and $M \otimes_R S$ is a finitely generated (resp. of finite presentation) S-module, then M is finitely generated (resp. of finite presentation) as R-module.

We include some results on finiteness conditions related to extension and restriction of scalars.

Proposition A.27. *Let $R \to S$ be an homomorphism of rings and let M be an S-module.*

(1) If M is finitely generated as R-module, then M is finitely generated as S-module.

(2) If M has finite presentation as R-module and S is finitely generated as R-module, then M has finite presentation as S-module.

Proof. (1) It follows from the fact that any generating system of M as an R-module is in particular a generating system of M as S-module, because the R-module structure of M is induced by the map $R \to S$.

(2) Since M has finite presentation as R-module, it is clear that M is finitely generated over R. By (1), M is also finitely generated as S-module. Thus, there is an exact sequence of S-modules $0 \to K \to S^n \to M$ for some positive integer n and an S-module K. This sequence can be considered as an exact sequence of R-modules by restriction of scalars. Since M has finite presentation as R-module and S^n is finitely generated as R-module, it follows from Proposition A.25.(3) that K is finitely generated as an R-module. Hence, (1) implies that K is finitely generated as an S-module and we conclude that M has finite presentation as S-module. □

Proposition A.28. *Let $R \to S$ be an homomorphism of rings such that S is finitely generated (resp. of finite presentation) as R-module. If M is a finitely generated (resp. of finite presentation) S-module, then the R-module M obtained by restriction of scalars is finitely generated (resp. of finite presentation).*

Proof. Case of finitely generated modules. We have surjections $S^n \to M$ and $R^m \to S$ for some positive integers m, n. Thus, we have a surjection $R^{mn} \to M$ and M is finitely generated as R-module.

Case of finite presentation modules. There is a short exact sequence of S-modules $0 \to K \to S^n \to M \to 0$, for some positive integer n and a finite S-module K. We can consider this sequence as an exact sequence of R-modules by restriction of scalars. Then S^n is finitely presented as R-module and K is finite as R-module, because S has finite presentation over R. Thus, by Proposition A.25, we conclude that M has finite presentation as R-module. □

On direct summands and free modules

We first recall some notions related to direct summands.

A.29. *Direct summand.* Let M be an R-module and let $N \subseteq M$ be a submodule. We say that N is a *direct summand* of M if there exists another submodule N' such that $M = N \oplus N'$. Equivalently, N is a direct summand of M if and only if the exact sequence of R-modules $0 \to N \to M \to M/N \to 0$ splits.

Lemma A.30 ([9, II, §3.4, Corollary 1]). *Let M be an R-module and let $N \subseteq M$ be a submodule such that M/N has finite presentation over R. Then N is a direct summand of M as R-module if and only if $N_\mathfrak{p}$ is a direct summand of $M_\mathfrak{p}$ as $R_\mathfrak{p}$-module for all $\mathfrak{p} \in \operatorname{Spec}(R)$.*

Now we review some concepts related to free modules over a ring.

A.31. *Free modules.* Let M be an R-module and Λ some set. Denote $R^{(\Lambda)} := \bigoplus_{\lambda\in\Lambda} R$.

- A subset $\{t_\lambda : \lambda \in \Lambda\} \subseteq M$ is a *system of generators* for M as R-module if the map $\bigoplus_{\lambda\in\Lambda} R \cdot t_\lambda \to M$ is a surjection.
- A collection $(t_\lambda)_{\lambda\in\Lambda} \subset M$ is a *basis* for M as R-module if the map $\bigoplus_{\lambda\in\Lambda} R\cdot t_\lambda \to M$ is an isomorphism.
- M is *free* if there exists an isomorphism $R^{(\Lambda)} \to M$, In this case, we say that M has *rank* the cardinality of Λ, which is uniquely determined by M.
- The collection $(e_\lambda)_{\lambda\in\Lambda}$, where $e_\lambda \in R^{(\Lambda)}$ is the element whose μ-th entry is $\delta_{\lambda\mu}$ for all $\lambda, \mu \in \Lambda$, is called the *standard basis* of $R^{(\Lambda)}$.

Since direct sums commute with tensor product, we have the following property for free modules.

Proposition A.32 ([8, §4.1, Corollary 9]). *Let $R \to S$ be an homomorphism of rings. If M is a free R-module, then $M \otimes_R S$ is also free as S-module.*

We recall some basic and well-known properties of finite free modules.

Proposition A.33. *Let M be a free R-module of finite rank n. Then*

(1) M is isomorphic to R^n as R-modules.

(2) The dual module $M^* := \operatorname{Hom}_R(M, R)$ is also free of finite rank n.

(3) There is a natural isomorphism of R-modules $M \simeq M^{**}$.

Proof. It is clear that if M is a free module of rank n, then there is an isomorphism $R^n \to M$ sending the standard basis of R^n into a basis $\{t_1, \ldots, t_n\}$ of M, that is, $e_i \mapsto t_i$ for each $i = 1, \ldots, n$. This proves (1). Moreover, for each element on the basis, we define $\varphi_i \colon M \to R$ such that $\varphi_i(x_1 t_1 + \ldots + x_n t_n) = x_i$. It is easy to show that $\varphi_1, \ldots, \varphi_n$ is a basis for M^* that we call the dual basis of $\{t_1, \ldots, t_n\}$. Thus, M^* is free of rank n as it is stated in (2). In particular, $M^* \simeq R^n$ by (1). Finally, we have $M^{**} = (M^*)^* \simeq (R^n)^* \simeq R^n \simeq M$ and the natural isomorphism in (3) is given by the map $M \to M^{**}$ that sends each element $m \in M$ into the evaluation map $\mathrm{ev}_m \colon M^* \to M$ defined by $\mathrm{ev}_m(\varphi) = \varphi(m)$. □

On Nakayama's Lemma

We enunciate the formulation of Nakayama's Lemma for finitely generated modules over a ring and its version over a local ring.

Lemma A.34 (Nakayama's Lemma, [8, §1.4, Lemma 10])**.** *Let M be a finitely generated R-module. Let $J(R)$ be the Jacobson radical ideal of R. If $I \subseteq J(R)$ is an ideal such that $IM = M$, then $M = 0$.*

Corollary A.35 (Local version of Nakayama's Lemma, [8, §1.4, Corollary 12])**.** *Let $(R, \mathfrak{m})$ be a local ring and let M be a finitely generated R-module. Then $m_1, \ldots, m_n \in M$ is a system of generators for M if and only if their images generate $M/\mathfrak{m}M$ as $R/\mathfrak{m}$-vector space. Moreover, $m_1, \ldots, m_n \in M$ is a minimal system of generators for M if and only if the images are a basis for $M/\mathfrak{m}M$ as $R/\mathfrak{m}$-vector space.*

We include some useful consequences of Nakayama's Lemma related to the generators of the finitely generated module.

Proposition A.36 ([47, Theorem 7.10])**.** *Let $(R, \mathfrak{m})$ be a local ring and let M be a flat R-module. If $x_1, \ldots, x_n \in M$ are such that their images in $M/\mathfrak{m}M$ are linearly independent over $R/\mathfrak{m}$, then $x_1, \ldots, x_n$ are linearly independent over R. In addition, assume that M is finite or $\mathfrak{m}$ is nilpotent. Then if $x_1, \ldots, x_n$ is also a minimal set of generators for M, then it is a basis and M is free.*

Corollary A.37. *Let R be a local ring and let M be a finitely generated R-module. Then M is free if and only if it is flat.*

Proof. We know that any finite free module is in particular flat. The converse in the local setting follows by a combination of Corollary A.35 and Proposition A.36. □

Proposition A.38. *Let M be a finitely generated R-module and let $\mathfrak{p} \subset R$ be a prime ideal. If $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module, then there are $x_1, \ldots, x_n \in M$ whose images in $M_\mathfrak{p}$ are a basis for $M_\mathfrak{p}$ as $R_\mathfrak{p}$-module.*

Proof. Let $x_1, \ldots, x_s \in M$ be a system of generators for M as R-module. Then the images in $M_\mathfrak{p}$ are a system of generators for $M_\mathfrak{p}$ as $R_\mathfrak{p}$-module. Moreover, the

classes of $x_1, \dots, x_s$ module $\mathfrak{p}M_\mathfrak{p}$ generate $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$ as a $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$-vector space. After rearrangement if necessary, we can choose $x_1, \dots, x_n$ such that their images in $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$ are a basis. Since $R_\mathfrak{p}$ is a local ring with maximal $\mathfrak{p}$ and $M_\mathfrak{p}$ is a finite flat $R_\mathfrak{p}$-module, we conclude by Proposition A.36 that $x_1, \dots, x_n \in M$ induce a basis for $M_\mathfrak{p}$ as $R_\mathfrak{p}$-module. □

Proposition A.39. *Let R be a local ring and let M be a finitely generated R-module. Let S be a generating set for M. If $\{x_1, \dots, x_s\} \subseteq S$ are part of a minimal generating set for M, then $\{x_1, \dots, x_s\}$ can be completed to a minimal generating set for M by adding elements of S. In addition, if M is flat, then M is free and $\{x_1, \dots, x_s\} \subseteq S$ are part of a basis for M and can be completed to a basis for M by adding elements of S.*

Proof. Denote by $\mathfrak{m}$ the maximal ideal of the local ring R and by $\bar{x}$ the class of an element $x \in M$ in $M/\mathfrak{m}M$. We assume first that $\{x_1, \dots, x_s\} \subseteq S$ are part of a minimal generating set for M. By Corollary A.35, the classes $\bar{x}_1, \dots, \bar{x}_s$ are a $R/\mathfrak{m}$-linearly independent subset of $M/\mathfrak{m}M$ and the classes of S generate $M/\mathfrak{m}M$ as an $R/\mathfrak{m}$-vector space. Then there are elements $\bar{x}_{s+1}, \dots, \bar{x}_n \in S$ such that $\{\bar{x}_1, \dots, \bar{x}_s, \bar{x}_{s+1}, \dots, \bar{x}_n\}$ is a basis for $M/\mathfrak{m}M$. Thus, by Corollary A.35, we conclude that $\{x_1, \dots, x_n\}$ is a minimal generating set for M as R-module. In addition, assume that M is flat, then by Proposition A.36 the R-module M is free and $\{x_1, \dots, x_s, x_{s+1}, \dots, x_n\}$ is a basis. □

A.3. Some properties of algebras

In this subsection, we collect some basic definitions and properties about algebras over a ring. Given an homomorphism of rings $\varphi\colon R \to S$, we say that S is an *R-algebra*. When it is clear, we omit the homomorphism φ from the notation and denote xy instead of $\varphi(x)y$ for each $x \in R$ and $y \in S$. Any R-algebra S is in particular an R-module.

A.40. *Finiteness conditions.* Let S be an R-algebra.

- S is *finite* if S is finitely generated as R-module.
- S is *finitely generated* if there exists a surjective homomorphism of R-algebras $R[X_1, \dots, X_n] \to S$.
- S is *of finite presentation* if there exists a surjective homomorphism of R-algebras $R[X_1, \dots, X_n] \to S$ whose kernel is finitely generated ideal.

Note that every finite R-algebra and every R-algebra of finite presentation is finitely generated. Moreover, any finite R-algebra is of finite presentation as R-module if and only if it is of finite presentation as R-algebra (see [24, Proposition B.12]).

We include some results related to the above finiteness properties of algebras.

Proposition A.41 ([24, Proposition B.10]). *Let $A \to B \to C$ be homomorphisms of rings.*

(1) If C has finite presentation as B-algebra and B has finite presentation as A-algebra, then C is an A-algebra of finite presentation.

(2) If C is an A-algebra of finite presentation and B is a finitely generated A-algebra, then C is a B-algebra of finite presentation.

Proposition A.42 ([24, Lemma B.9 and Proposition B.52]). *Let R_0 be a ring. Let $(R_\lambda)_{\lambda\in\Lambda}$ be a filtered inductive system of R_0-algebras and set $R = \varinjlim R_\lambda$.*

(1) If S is an R-algebra of finite presentation, then there exists $\lambda \in \Lambda$ and an R_λ-algebra S_λ of finite presentation such that $S = S_\lambda \otimes_{R_\lambda} R$.

(2) If S_0 is an R_0-algebra of finite presentation such that $S := R \otimes_{R_0} S_0$ is a finite R-algebra, then there exists $\lambda \in \Lambda$ such that the R_λ-algebra $S_\lambda := R_\lambda \otimes_{R_0} S_0$ is finite.

Bibliography

[1] M. André. Homologie de Frobenius. *Mathematische Annalen*, 290:129–181, 1991.

[2] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, Reading, Mass.-London-Don Mills, Ont., Reprint edition, 1969.

[3] L. L. Avramov. Homology of local flat extensions and complete intersection defects. *Mathematische Annalen*, 228(1):27–37, 1977.

[4] V. V. Bavula. Simple derivations of differentiably simple Noetherian commutative rings in prime characteristic. *Transactions of the American Mathematical Society*, 360(8):4007–4027, 2008.

[5] L. Bégueri. Schéma d'automorphisms. Application à l'étude d'extensions finies radicielles. *Bulletin des Sciences Mathématiques. 2e Série*, 93(1):89–111, 1969.

[6] R. E. Block. Differentiably simple algebras. *Bulletin of the American Mathematical Society*, 74(6):1086–1090, 1968.

[7] R. E. Block. Determination of the differentiably simple rings with a minimal ideal. *The Annals of Mathematics. Second Series*, 90(3):433–459, 1969.

[8] S. Bosch. *Algebraic Geometry and Commutative Algebra*. Universitext. Springer London, 1 edition, 2012.

[9] N. Bourbaki. *Elements of mathematics. Commutative algebra*. Hermann, Paris; Addison-Wesley Publishing Company, Reading, MA, 1972. Translated from the French.

[10] L. Brantner and J. Waldron. Purely Inseparable Galois theory I: The Fundamental Theorem. *arXiv preprint arXiv:2010.15707*, 2023.

[11] C. del Buey de Andrés and D. Sulca. Purely Inseparable extensions of rings. *arXiv preprint arXiv:2407.01056*, 2024.

[12] C. del Buey de Andrés, D. Sulca, and O. E. Villamayor. Differentiably simple rings and ring extensions defined by p-basis. *Journal of Pure and Applied Algebra*, 228(12), 2024.

[13] H. Cartan. Théorie de Galois pour les corps non commutatifs. *Annales Scientifiques de l'École Normale Supérieure. Troisième Série*, 64:59–77, 1947.

[14] H. Cartan and S. Eilenberg. *Homological Algebra.* Princeton University Press, Princeton, NJ. Princeton Mathematical Series, 1956.

[15] S. U. Chase. On inseparable Galois theory. *Bulletin of the American Mathematical Society*, 77(3):413–417, 1971.

[16] S. U. Chase. On the automorphism scheme of a purely inseparable field extension. In R. Gordon, editor, *Ring Theory. Proceedings of a Conference on Ring Theory held in Park City, Utah, March 2–6, 1971.* Academic Press Inc., 1972.

[17] S. U. Chase. Infinitesimal Group Scheme Actions on Finite Field Extensions. *American Journal of Mathematics*, 98(2):441–480, 1976.

[18] M. Demazure and G. P. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs.* Masson & Cie, Éditeurs, Paris; North-Holland Publishing Co., Amsterdam, 1970.

[19] D. Farkas, C. Geiss, and E. Marcos. Smooth automorphism group schemes. *in Representations of algebras, Lecture Notes in Pure and Applied Mathematics*, 224:71–89, 2002.

[20] J. Feng, R. Shen, and J. Zhang. Jacobson-Bourbaki Correspondence Theorem for Noncommutative rings. *Journal of Donghua University (English Edition)*, 36:23–26, 2019.

[21] H. Fitting. Die Determinantenideale eines Moduls. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 46:195–228, 1936.

[22] M. Gerstenhaber. On modular field extensions. *Journal of Algebra*, 10(4):478–484, 1968.

[23] M. Gerstenhaber and A. Zaromp. On the Galois theory of purely inseparable field extensions. *Bulletin of the American Mathematical Society*, 76(3):1011–1014, 1970.

[24] U. Görtz and T. Wedhorn. *Algebraic Geometry I: Schemes with examples and exercises.* Vieweg+Teubner, 1st edition, 2010.

[25] A. Grothendieck. *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. IV*, volume 32. Institut des Hautes Études Scientifiques. Publications Mathématiques, 1967.

[26] A. Grothendieck and J. Dieudonné. *Eléments de géometrie algébrique I.* Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1971.

[27] L. Gruson and M. Raynaud. Critères de platitude et de projectivité. Techniques de "platification" d'un module. *Inventiones mathematicae*, 13:1–89, 1971.

[28] T. Gulliksen and G. Levin. Homology of local rings. *Queen's Papers in Pure and Applied Mathematics*, 20, 1969.

[29] L. R. Harper, Jr. On differentiably simple algebras. *Transactions of the American Mathematical Society*, 100:63–72, 1961.

[30] N. Heerema and D. Tucker. Modular field extensions. *Proceedings of the Mathematical American Society*, 53(2):301–306, 1975.

[31] G. Hochschild. Double vector spaces over division rings. *American Journal of Mathematics*, 71(2):443–460, 1949.

[32] G. Hochschild. Simple algebras with purely inseparable splitting fields of exponent 1. *American Journal of Mathematics*, 79:477–489, 1955.

[33] A. Holleman. Inseparable Algebras. *Journal of Algebra*, 46(2):415–429, 1977.

[34] N. Jacobson. Abstract Derivation and Lie Algebras. *American Journal of Mathematics*, 42(2):206–224, 1937.

[35] N. Jacobson. An extension of Galois theory to non-normal and non-separable fields. *American Journal of Mathematics*, 66(1):1–29, 1944.

[36] N. Jacobson. Galois theory of purely inseparable fields of exponent one. *American Journal of Mathematics*, 66(4):645–648, 1944.

[37] N. Jacobson. A note on division rings. *American Journal of Mathematics*, 69(1):27–36, 1947.

[38] N. Jacobson. *Lectures in Abstract Algebra, III. Theory of Fields and Galois Theory*. Graduate Texts in Mathematics. Springer-Verlag, Reprint edition, 1964.

[39] I. Kaplansky. Projective Modules. *Annals of Mathematics. Second Series*, 68(2):372–377, 1958.

[40] T. Kimura and H. Niitsuma. On Kunz's conjecture. *Journal of the Mathematical Society of Japan*, 34(2):371–378, 1982.

[41] T. Kimura and H. Niitsuma. Differential Basis and p-Basis of a Regular Local Ring. *Proceedings of the American Mathematical Society*, 92(3):335–338, 1984.

[42] H. F. Kreimer and N. Heerema. Modularity vs. Separability for Field Extensions. *Canadian Journal of Mathematics*, 27(5):1176–1182, 1975.

[43] E. Kunz. Almost complete intersections are not Gorenstein rings. *Journal of Algebra*, 28:111–115, 1974.

[44] E. Kunz. *Kähler differentials*. Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden GmbH, 1986.

[45] T. Lam. *Exercises in modules and rings*. Problem Books in Mathematics. Springer, 2007.

[46] A. K. Maloo. Generators for a maximally differential ideal in positive characteristic. *Nagoya Mathematical Journal*, 132:37–41, 1993.

[47] H. Matsumura. *Commutative ring theory*, volume 8 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 1989.

[48] J. S. Milne. *Algebraic groups: the theory of group schemes of finite type over a field*. Cambridge University Press, 2017.

[49] F. Pauer. Spezielle Algebren und transitive Operationen. *Mathematische Zeitschrift*, 160(2):103–134, 1978.

[50] A. Perry. Faithfully flat descent for projectivity of modules. *ArXiv preprint arxiv: 1011.0038v1*, 2010.

[51] G. Pickert. Eine Normalform für endliche rein-inseparable Körpererweiterungen. *Mathematische Zeitschrift*, 53:133–135, 1950.

[52] G. Pickert. Inseparable Körpererweiterungen. *Mathematische Zeitschrift*, 52:81–136, 1950.

[53] E. C. Posner. Differentiably simple rings. *Proceedings of the American Mathematical Society*, 11:337–343, 1960.

[54] R. Rasala. Inseparable Splitting Theory. *American Journal of Mathematics*, 162:411–448, 1971.

[55] F. Sancho de Salas and P. J. Sancho de Salas. Desingularization and integrality of the automorphism scheme of a finite field extension. *Mathematische Zeitschrift*, 233(2):305–325, 2000.

[56] P. Sancho de Salas. Differentially Homogeneous Algebras. *Journal of Algebra*, 216(2):620–640, 1999.

[57] S. Satô. On Purely Inseparable Algebras and P.H.D. rings. *Transactions of the American Mathematical Society*, 266(2):483–498, 1981.

[58] S. Satô. Modular extensions. *Proceedings of the American Mathematical Society*, 109(3):621–626, 1990.

[59] J.-P. Serre. Modules projectifs et espaces fibrés à fibre vectorielle. *Séminaire Dubreil. Algèbre et théorie des nombres*, 11(2):Talk no. 23, 1957-1958.

[60] S. Shatz. Galois theory. In P. Hilton, editor, *Category Theory, Homology Theory and their Applications I*, volume 86 of *Lecture Notes in Mathematics*. Springer-Verlag, 1969.

[61] M. Sweedler. Purely Inseparable Algebras. *Journal of Algebra*, 35(1):342–355, 1975.

[62] M. E. Sweedler. Structure of Inseparable Extensions. *Annals of Mathematics*, 87(3):401–410, 1968.

[63] J. Tate. Homology of Noetherian rings and local rings. *Illinois Journal of Mathematics*, 1(1):14–27, 1957.

[64] M. Wechter. Differential operators on modular extensions. *Journal of Commutative Algebra*, 7(3):447–458, 2015.

[65] D. Winter. A Galois theory of commutative rings. *Journal of Algebra*, 289:380–411, 2005.

[66] S. Yuan. Differentiably simple rings of prime characteristic. *Duke Mathematical Journal*, 31(4):623–630, 1964.

[67] S. Yuan. Finite dimensional inseparable algebras. *Transactions of the American Mathematical Society*, 150(2):577–587, 1970.

[68] S. Yuan. Inseparable Galois theory of exponent one. *Transactions of the American Mathematical Society*, 149(1):163–170, 1970.