Rational actions of infinitesimal group schemes

Bianca Gouthier

THÈSE

PRÉSENTÉE POUR OBTENIR LE GRADE DE

DOCTEURE DE L'UNIVERSITÉ DE BORDEAUX

École Doctorale de Mathématiques et d'Informatique
Spécialité : Mathématiques pures

par **Bianca GOUTHIER**

Actions rationnelles de schémas en groupes infinitésimaux

Sous la direction de **Dajano TOSSICI**

Soutenue le 2 juillet 2024 à l'Institut de Mathématiques de Bordeaux.

Membres du jury :

M. Michel BRION	Professeur, Université Grenoble Alpes	Rapporteur
M. Matthieu ROMAGNY	Professeur, Université de Rennes	Rapporteur
M. Qing LIU	Professeur, Université de Bordeaux	Président
Mme Alessandra BERTAPELLE	Professeure adjointe, Università degli Studi di Padova	Examinatrice
M. Xavier CARUSO	Directeur de recherche, Université de Bordeaux	Examinateur
Mme Valentijn KAREMAKER	Professeure adjointe, Universiteit Utrecht	Examinatrice
M. Stefan SCHRÖER	Professeur, Universität Düsseldorf	Examinateur
M. Dajano TOSSICI	Maître de conférence, Université de Bordeaux	Directeur de thèse

Actions rationnelles de schémas en groupes infinitésimaux

Résumé : Cette thèse porte sur l'étude des actions (rationnelles) des schémas en groupes infinitésimaux, avec un accent particulier sur les schémas en groupes infinitésimaux commutatifs unipotents et les actions génériquement libres et les actions fidèles. Pour tout k-schéma en groupes fini G agissant rationnellement sur une k-variété X, si l'action est génériquement libre, alors la dimension de l'algèbre $\mathrm{Lie}(G)$ est majorée par la dimension de la variété. Nous montrons que c'est la seule obstruction lorsque k est un corps parfait de caractéristique positive et que G est infinitésimal commutatif trigonalisable. Si G est unipotent, nous montrons aussi que toute action rationnelle génériquement libre sur X du noyau de (toute puissance du) Frobenius de G s'étend à une action rationnelle génériquement libre de G sur X. De plus, nous donnons des conditions nécessaires pour avoir des actions rationnelles fidèles de schémas en groupes infinitésimaux commutatifs trigonalisables sur des variétés, et des conditions suffisantes (différentes) dans le cas unipotent sur un corps parfait.

L'étude des actions fidèles des schémas en groupes sur une variété X fournit des informations sur les sous-groupes représentables du foncteur-groupe des automorphismes Aut_X de X. Pour tout corps k, $\mathrm{PGL}_{2,k}$ représente le foncteur-groupe des automorphismes de $\mathbb{P}^1_k$ et donc les sous-schémas en groupes de $\mathrm{PGL}_{2,k}$ correspondent aux actions fidèles sur $\mathbb{P}^1_k$. De plus, $\mathrm{PGL}_{2,k}(k)$ coïncide avec le groupe de Cremona en dimension un, c'est-à-dire les morphismes birationnels de $\mathbb{P}^1_k$, puisque toute application rationnelle d'une courbe projective non singulière dans elle-même s'étend à la courbe entière. En caractéristique positive, la situation est complètement différente si l'on considère les actions rationnelles de schémas en groupes infinitésimaux. La plupart des actions infinitésimales fidèles sur la droite affine ne s'étendent pas à $\mathbb{P}^1_k$. Si la caractéristique d'un corps k est impaire, tout sous-schéma en groupes infinitésimal de $\mathrm{PGL}_{2,k}$ se relève à $\mathrm{SL}_{2,k}$. Ceci n'est pas vrai en caractéristique 2 et, dans ce cas, nous donnons une description complète, à isomorphisme près, des sous-schémas en groupes infinitésimaux unipotents de $\mathrm{PGL}_{2,k}$.

Enfin, nous prouvons un résultat qui donne une description explicite de tous les k-schémas en groupes infinitésimaux commutatifs unipotents avec algèbre de Lie unidimensionnelle définis sur un corps algébriquement clos k, montrant qu'il y a exactement n tels schémas en groupes non isomorphes d'ordre fixé p^n.

Mots-clés : *schémas en groupes ; actions rationnelles ; torseurs ; algèbres de Hopf ; opérateurs différentiels ; algèbre de Lie ; smash product.*

Institut de Mathématiques de Bordeaux
UMR 5251, Université de Bordeaux, 351 cours de la Libération, 33405 Talence, France.

Rational actions of infinitesimal group schemes

Abstract: This thesis focuses on the study of (rational) actions of infinitesimal group schemes, with a particular emphasis on infinitesimal commutative unipotent group schemes and generically free actions and faithful actions. For any finite k-group scheme G acting rationally on a k-variety X, if the action is generically free then the dimension of $\mathrm{Lie}(G)$ is upper bounded by the dimension of the variety. We show that this is the only obstruction when k is a perfect field of positive characteristic and G is infinitesimal commutative trigonalizable. If G is unipotent, we also show that any generically free rational action on X of (any power of) the Frobenius kernel of G extends to a generically free rational action of G on X. Moreover, we give necessary conditions to have faithful rational actions of infinitesimal commutative trigonalizable group schemes on varieties, and (different) sufficient conditions in the unipotent case over a perfect field.

Studying faithful group scheme actions on a variety X yields information on representable subgroups of the automorphism group functor Aut_X of X. For any field k, $\mathrm{PGL}_{2,k}$ represents the automorphism group functor of $\mathbb{P}^1_k$ and thus subgroup schemes of $\mathrm{PGL}_{2,k}$ correspond to faithful actions on $\mathbb{P}^1_k$. Moreover, $\mathrm{PGL}_{2,k}(k)$ coincides with the Cremona group in dimension one, i.e. birational self-maps of $\mathbb{P}^1_k$, since any rational self-map of a projective non-singular curve extends to the whole curve. In positive characteristic, the situation is completely different if we consider rational actions of infinitesimal group schemes. Most of the faithful infinitesimal actions on the affine line do not extend to $\mathbb{P}^1_k$. If the characteristic of a field k is odd, any infinitesimal subgroup scheme of $\mathrm{PGL}_{2,k}$ lifts to $\mathrm{SL}_{2,k}$. This is not true in characteristic 2 and, in this case, we give a complete description, up to isomorphism, of infinitesimal unipotent subgroup schemes of $\mathrm{PGL}_{2,k}$.

Finally, we prove a result that gives an explicit description of all infinitesimal commutative unipotent k-group schemes with one-dimensional Lie algebra defined over an algebraically closed field k, showing that there are exactly n non-isomorphic such group schemes of fixed order p^n.

Keywords: *group schemes; rational actions; torsors; Hopf algebras; differential operators; Lie algebra; smash products.*

Acknowledgements

I would like to start by thanking my supervisor Dajano Tossici: thank you for guiding me through the years of my PhD, I am very grateful for all the time you consacrated to discussing Maths with me and to my thesis. I consider myself lucky for finding, over all these years, your door always open for me to come in and ask questions.

I am very thankful to Michel Brion and Matthieu Romagny for carefully reading my thesis and for their helpful comments that led to a better version of this work. Thanks also to Alessandra Bertapelle, Valentijn Karemaker, Stefan Schröer for accepting of being part of my jury together with Xavier Caruso and Qing Liu that I thank moreover for the discussions and the support over these years.

Merci à tous les membres de l'équipe de Théorie des Nombres, ça a été un vrai plaisir d'en faire partie.

Merci à Cyril, pour le bonheur qu'il donne à la BMI et pour sa disponibilité et travail pour nous faire avoir des ouvrages depuis toute la France. Merci à Ida, pour la patience et l'aide dans l'organisation de toutes les missions de ces années. Merci à Karine, pour son soutien et toute les propositions de course à Bordeaux, mais surtout pour ses souris et bonne humeur.

Grazie Jasmin, il tuo arrivo all'IMB è stato una folata d'allegria e di tante chiacchere. Grazie per il supporto e i consigli che hai avuto per me in questi anni!

Grazie Elena, per la tua amicizia, la tua energia e per condividere la tua esperienza di giovane matematica.

Merci Théo : ton amitié a été déterminant dès notre année de Master pour ma vie a Bordeaux. Merci pour le temps partagé en temps difficiles en début de thèse, pour avoir été un très bon cobureau, un très très bon exemple de personne passionnée par les maths et un encore plus bon ami !

Merci Paul : un des jours meilleurs de ma première année de thèse à surement été le jour où je t'ai proposé de me rejoindre au Voltaire en colocation. Merci pour ta patience à jouer au tennis avec moi quand je savais à peu près que taper la balle. Merci pour tout le temps passé ensemble, à papoter, à regarder des series, à s'écouter. T'as été un super colocataire et tu restera toujours un très bon ami.

Grazie Nicoletta, per esserci stata all'inizio del mio percorso di dottorato, per il supporto reciproco che continua a distanza e per il tempo che abbiamo potuto passare assieme a Bordeaux.

Grazie Marco, per portare energia ovunque con te! Sei stato un ottimo compagno

di ufficio e coinquilino. Grazie per esserci sempre per riflettere insieme a domande matematiche e per la quotidiana condivisione di alti e bassi di questi anni. Ti auguro una buona fine di tesi e un brillante futuro.

Merci Agathe, même si quand on s'est connues tu ne me disais même pas bonjour (oui oui, tu dis que je te faisais peur...), je suis très ravie de comment on est devenues amies au passer des années. T'as été une cobureaue fantastique ! Merci pour ta présence, ton aide et ton soutien.

Merci à tout.e.s les doctorant.e.s que j'ai pu croiser pendant mes années à l'IMB, ce qui étaient là quand je suis arrivée et ce qui resteront maintenant que je pars. Merci pour les moments de convivialité et les repas partagés et pour alimentaire une belle atmosphère de jeunesse et d'allégresse.

Un grand merci à Alexa : à part avoir appris un peu plus de maths je vais repartir de Bordeaux en ayant aussi appris à jouer au tennis ! Merci pour tous les cours particuliers le lundi à 8h30 qui donnaient tout un autre goût à mon début de semaine, pour ton intérêt vers mon travail, mes voyages et l'Italie. Merci aussi car tu m'as fait connaître Anna ! Bizzarro ritrovarsi dal Friuli a Bordeaux su un campo da tennis. Grazie Annina per la tua amicizia e per il tempo trascorso a Bordeaux insieme, giocando a tennis, passeggiando, discutendo e facendo aperitivi ad alta quota.

Grazie ai Magici Fra, Luca, Fabi e Mame, perché il tempo trascorso con voi è sempre facile e genuino: è molto bello vedere come la nostra amicizia si evolve, trasforma e rafforza col passare degli anni. Siete stati degli ottimi compagni di dottorato a distanza, grazie del vostro supporto e della vostra presenza. Un rigranziamento speciale va a Mame: grazie per aver vissuto fianco a fianco assieme a me questi anni di dottorato. Grazie per le settimane e settimane trascorse un po' in Francia, un po' in Olanda a imparare insieme da casa nel periodo del covid, per le ore di ascolto e condivisione su lavagne virtuali e non, per essere un esempio di curiosità e coraggio, per tutti i primi passi nel mondo accademico fatti assieme, per le conferenze in giro per il mondo che vissute insieme hanno tutto un altro gusto e per tutte le avventure di contorno, per il tuo supporto e la tua stima incondizionati, per gioire in modo genuino di ogni mio traguardo. Senza tutto ciò in questi anni avrei imparato un decimo della matematica e fatto un centesimo delle cose. Spronanarci a vicenda è stato determinante per il raggiungimento di questo traguardo.

Grazie ai miei amici di casa, Moreno, Giulia, Zorz, Paolo, Elisa: è bello ritrovarvi a ogni mio passaggio in FVG. Giulia, ancora non ti sei stancata di ascoltare mie presentazioni poco comprensibili, grazie per essere qui anche in questa occasione!

Grazie alla mia famiglia, grazie mamma, papà, Somu, Anshi e Alberto per la vostra stima e affetto, per accettare il fatto che io sia lontana e per esserci ogni volta in cui torno. Grazie ai nonni Beppe e Marisa per essere sempre interessati ai miei passi successivi, a nonna Anna che "poi l'hai finita di studiare?", a nonno Lino che sento sempre vicino nel cuore, a zio Umberto, esempio di curiosità, con il suo seguirmi per il mondo e la sua immancabile domanda "ma io cosa dovrei fare per riuscire a capire quello che fai?".

L'ultimo di questi grazie va alla persona più presente al mio fianco: grazie Antonio per essermi sempre accanto, per il tuo supporto, i tuoi incoraggiamenti, per ricordarmi a ogni passo e traguardo che credi in me e sei orgoglioso di me.

Résumé substantiel en français

Cette thèse se concentre sur l'étude des actions (rationnelles) des schémas en groupes infinitésimaux, avec un accent particulier sur les schémas en groupes infinitésimaux commutatifs unipotents et sur les actions génériquement libres et les actions fidèles. Ces schémas en groupes n'existent qu'en caractéristique positive et des exemples apparaissent en regardant la p-torsion des variétés abéliennes.

L'intérêt pour ce sujet a de multiples motivations. Soit k un corps et X un k-schéma. Le foncteur en groupes des automorphismes Aut_X de X qui associe à tout k-schéma S le groupe des S-automorphismes $\mathrm{Aut}_S(X \times_k S)$ n'est pas représentable en général. Cet objet a été largement étudié : on sait par exemple que si X est propre, alors Aut_X est un k-schéma en groupes localement de type fini [MO67]. Si K/k est une extension finie purement inséparable, le schéma en groupes des automorphismes $\mathrm{Aut}_K := \mathrm{Aut}_{\mathrm{Spec}(K)}$ a été étudié par exemple par [Beg69] et [Cha72].

Pour G un k-schéma en groupes, il existe une bijection entre les G-actions $G \times_k X \to X$ sur X et les homomorphismes de foncteurs en groupes $G \to \mathrm{Aut}_X$. Si l'action de G est fidèle, alors G est un sous-foncteur en groupes de Aut_X. L'étude des actions fidèles des schémas en groupes fournit alors des informations sur les sous-groupes représentables de Aut_X. Lorsque Y est le point générique d'une variété X (schéma séparé, géométriquement intègre de type fini) et que G est un k-schéma en groupes fini, se donner une G-action sur $Y = \mathrm{Spec}(k(X))$ équivaut à se donner une G-action rationnelle sur X. L'étude de telles actions rationnelles fidèles apporte alors des connaissances sur le foncteur en groupes des automorphismes Aut_K des extensions séparables finiment engendrées K/k.

Lorsque $K = k(t_1, \ldots, t_n)$ est une extension transcendante pure de k, alors $\mathrm{Aut}_K(k)$ coïncide avec le groupe de Cremona $\mathrm{Cr}_n(k) = \mathrm{Bir}_k(\mathbb{P}^n_k)$ en dimension n, qui est par définition le groupe des automorphismes birationnels de $\mathbb{P}^n_k$. Le groupe de Cremona a été profondément étudié en caractéristique zéro, alors qu'il a été moins étudié en caractéristique positive (voir par exemple l'étude [Dol10]). Dolgachev a formulé la conjecture suivante pour le groupe de Cremona sur un corps de caractéristique positive.

Conjecture. Si k est un corps de caractéristique $p > 0$, le groupe de Cremona $\mathrm{Cr}_n(k)$ ne contient pas d'élément d'ordre p^s pour $s > n$ [Dol10, Conjecture 37].

La conjecture est vraie pour $n = 1$ puisque $\mathrm{PGL}_2(k) \simeq \mathrm{Aut}_k(k(t))$ ne contient pas d'élément d'ordre p^2 si $car(k) = p > 0$. De plus, cette conjecture a été prouvée pour $n = 2$ [Dol09]. La conjecture peut être reformulée de la manière suivante : s'il existe une

action rationnelle fidèle d'un p-groupe commutatif fini G sur $\mathbb{P}^n_k$ alors $p^n_G = 0$, où p_G est le morphisme de multiplication par p sur G. En effet, il existe une correspondance bijective naturelle entre les actions fidèles d'un p-groupe commutatif fini G sur $k(t_1, \ldots, t_n)$ et les actions rationnelles fidèles du schéma en groupes constant correspondant sur $\mathbb{P}^n_k$.

Dans cette thèse, nous nous intéressons aux actions rationnelles des schémas en groupes infinitésimaux. L'analogue de la conjecture de Dolgachev pour les schémas en groupes unipotents commutatifs infinitésimaux apparaît naturellement de l'une des manières suivantes : si k est un corps de caractéristique $p > 0$ et G est un k-schéma en groupes infinitésimal commutatif unipotent, s'il existe une action rationnelle fidèle de G sur $\mathbb{P}^n_k$, alors $p^n_G = 0$ (ou peut-être $V^n_G = 0$, où V_G est le morphisme de décalage de G). Les deux options s'avèrent fausses. En effet, par exemple, toute courbe admet des actions rationnelles fidèles de la p^n-torsion $E[p^n]$ d'une courbe elliptique supersingulière E (puisque dans ce cas $E[p^n]$ est un k-schéma en groupes infinitésimal commutatif unipotent avec algèbre de Lie unidimensionnelle et donc le Théorème 1 s'applique) mais $V_{E[p^n]} \neq 0$, et $p_{E[p^n]} \neq 0$ si $n > 1$.

Ce qui est vrai, c'est que s'il existe une action rationnelle fidèle de G sur une k-variété de dimension n, alors $V^n_{\ker(F_G)} = 0$. Nous donnons une preuve de ce résultat dans la section 3.3 du chapitre 3. L'implication inverse n'est pas toujours vraie : nous montrons que par exemple il n'existe pas d'action rationnelle fidèle de la p-torsion d'une variété abeliénne superspéciale de dimension au moins 2 sur des courbes. De plus, nous montrons qu'il existe des actions rationnelles fidèles de tout schéma en groupes infinitésimal commutatif unipotent G défini sur un corps parfait sur toute variété de dimension n si $V^n_G = 0$.

Nous nous intéressons plus précisément aux actions rationnelles qui sont génériquement libres. En effet, en caractéristique positive, toutes les actions fidèles n'admettent pas un sous-ensemble ouvert et dense $U \subseteq X$ qui soit G-stable et tel que l'action de G sur U soit libre. Pour tout k-schéma en groupes fini G agissant rationnellement sur une k-variété X, si l'action est génériquement libre, alors la dimension de l'algèbre de Lie de G $\mathrm{Lie}(G)$ est majorée par la dimension de la variété. Dans l'un des principaux résultats de cette thèse, nous montrons que cette inégalité est la seule obstruction lorsque k est un corps parfait de caractéristique positive et que G est infinitésimal commutatif trigonalisable. Si G est unipotent, nous montrons aussi que toute action rationnelle génériquement libre sur X du noyau de (toute puissance du) Frobenius de G s'étend à une action rationnelle génériquement libre de G sur X.

Théorème 1. *Soit k un corps parfait de caractéristique $p > 0$ et G un k-schéma en groupes infinitésimal commutatif unipotent avec algèbre de Lie de dimension s. Alors pour toute k-variété X de dimension $\geq s$ il existe des actions rationnelles génériquement libres de G sur X. De plus, pour tout $r \geq 1$, toute action rationnelle génériquement libre de $\ker(F^r_G)$ sur X peut être étendue à une action rationnelle génériquement libre de G sur X.*

La preuve que nous donnons est constructive et permet d'écrire explicitement de telles actions : nous terminons la section 3.2 du chapitre 3 avec plusieurs exemples le montrant concrètement. La difficulté est de construire des actions en basse dimension, c'est-à-dire proche de la dimension de $\mathrm{Lie}(G)$.

Remarquons que si un k-schéma en groupes infinitésimal commutatif unipotent G avec algèbre de Lie de dimension n peut être plongé dans un groupe algébrique lisse connexe $\mathcal{G}$ de dimension n, alors G agit de manière génériquement libre sur $\mathcal{G}$ (par multiplication). Brion a demandé si, déjà dans le cas unidimensionnel, il y a des exemples différents qui apparaissent [Bri22] et de plus si ces schémas en groupes sont toujours commutatifs (voir aussi [Fak20, Remark 2.10]). Nous répondons à ces questions en montrant qu'il existe des actions rationnelles génériquement libres sur des courbes de schémas en groupes infinitésimaux commutatifs unipotents qui ne sont pas des sous-groupes d'un groupe algébrique unidimensionnel lisse et connexe et qu'il existe des actions rationnelles génériquement libres de schémas en groupes infinitésimaux non-commutatifs sur des variétés.

En général, il n'est pas facile de décrire explicitement les schémas en groupes unipotents commutatifs infinitésimaux. Par exemple, ceux qui proviennent de la p-torsion d'une variété abélienne (avec p-rang zéro) ne sont pas complètement compris et augmentent en complexité lorsque la dimension croît. Une description explicite de ces schémas en groupes, par exemple en termes de leur algèbre de Hopf, est utile pour construire des actions de ces schémas en groupes sur les variétés. Dans cette thèse, on donne une description explicite de tous les k-schémas en groupes infinitésimaux commutatifs unipotents avec algèbre de Lie unidimensionnelle définie sur un corps algébriquement clos k, répondant partiellement à une question de Fakhruddin (voir [Fak20, Remark 2.10]). Précisément, nous montrons que :

Théorème 2. *Si $k = \overline{k}$ est un corps de caractéristique $p > 0$, pour tout $n \geq 1$, il existe exactement n k-schémas en groupes infinitésimaux commutatifs unipotents non-isomorphes d'ordre p^n et avec algèbre de Lie unidimensionnelle. Il s'agit des schémas en groupes de la forme*

$$W_n^n[V - F^i] := \ker(V - F^i \colon W_n^n \to W_n^n)$$

pour $i = 1, \ldots, n$.

Ce résultat est connu pour les schémas en groupes infinitésimaux commutatifs unipotents d'ordre $\leq p^3$ grâce à [Oor66, (15.5)] et [NWW15, Théorème 1.1].

Parmi ces schémas en groupes, les seuls qui soient contenus dans un groupe algébrique unidimensionnel lisse et connexe sont α_{p^n} et $W_n^n[F - V]$ (le premier est un sous-schéma en groupes de $\mathbb{G}_a$ et le second est contenu dans la p^n-torsion d'une courbe elliptique supersingulière) pour tout $n \geq 1$. Tous les autres sont des exemples de schémas en groupes infinitésimaux qui agissent de manière génériquement libre sur toute courbe, mais ne sont pas des sous-schémas en groupes d'un groupe algébrique unidimensionnel lisse et connexe. En outre, $W_n^n[F - V]$ est le seul schéma en groupes self-dual de la liste. Si l'on considère des schémas en groupes infinitésimaux commutatifs unipotents avec algèbre de Lie de dimension supérieure, ce n'est plus le cas : en effet, la p-torsion de toute variété abélienne principalement polarisée de dimension g et de p-rang zéro, est un schéma en groupes infinitésimal commutatif unipotent, et il existe p^{g-1} classes d'isomorphisme différentes de telles variétés.

Fakhruddin a prouvé que si G est infinitésimal et Y est une courbe projective normale avec une action rationnelle de G, s'il existe une variété projective normale X avec une action de G et une application rationnelle dominante G-équivariante $X \dashrightarrow Y$, alors l'action rationnelle de G sur Y s'étend de façon unique à une action de G sur Y [Fak20, Proposition 2.2]. En particulier, dans la situation ci-dessus, si Y est la droite projective et que l'action est fidèle, alors G est un sous-schéma en groupes de $\mathrm{PGL}_{2,k}$. La plupart des schémas en groupes infinitésimaux unipotents avec algèbre de Lie unidimensionnelle ne sont pas contenus dans $\mathrm{PGL}_{2,k}$, mais pour tous ceux-ci, il existe des actions rationnelles génériquement libres sur la droite projective. Par conséquent, la plupart de ces actions rationnelles sur la droite projective ne sont pas induites par des actions, définies partout, sur des variétés normales projectives de dimension supérieure.

Si la caractéristique d'un corps k est impaire, tout sous-schéma en groupes infinitésimal de $\mathrm{PGL}_{2,k}$ se relève à $\mathrm{SL}_{2,k}$. Une partie de cette thèse est consacrée à montrer que ce n'est plus vrai en caractéristique 2 et nous donnons une description complète, à isomorphisme près, des sous-schémas en groupes infinitésimaux unipotents de $\mathrm{PGL}_{2,k}$. Nous considérons également le cas infinitésimal trigonalisable.

Dans son article [Bea10], Beauville a classifié, à conjugaison près, tous les sous-groupes finis de $\mathrm{PGL}_2(k)$ d'ordre premier à la caractéristique. Nous nous intéressons ici au cas opposé, les sous-schémas en groupes infinitésimaux. Il semble que ce soit un fait accepté que tout sous-schéma en groupes infinitésimal de $\mathrm{PGL}_{2,k}$ se relève à $\mathrm{GL}_{2,k}$. En particulier, tout sous-schéma en groupes infinitésimal unipotent de $\mathrm{PGL}_{2,k}$ serait un sous-schéma en groupes de $\mathbb{G}_{a,k}$, et il serait donc isomorphe à $\alpha_{p^n,k}$ pour un certain $n \geq 0$. Nous prouvons que ce n'est pas vrai si la caractéristique du corps est 2. Le résultat est par contre vrai si la caractéristique est impaire et nous en donnons une preuve.

Pour tout corps k, $\mathrm{PGL}_{2,k}$ représente le foncteur en groupes des automorphismes de $\mathbb{P}^1_k$. L'étude des sous-schémas en groupes correspond donc aux actions fidèles sur $\mathbb{P}^1_k$. De plus, $\mathrm{PGL}_{2,k}(k)$ coïncide avec le groupe de Cremona en dimension un, c'est-à-dire les transformations birationnelles de $\mathbb{P}^1_k$, puisque toute application rationnelle d'une courbe projective non-singulière s'étend à la courbe entière. En caractéristique positive, la situation est complètement différente si l'on considère les actions rationnelles des schémas en groupes infinitésimaux. La plupart des actions infinitésimales fidèles de la droite affine ne s'étendent pas à $\mathbb{P}^1_k$. Par exemple, toutes les actions fidèles de α_p^n, avec $n \geq 4$, sur $\mathbb{A}^1_k$ ne s'étendent pas à $\mathbb{P}^1_k$, puisque $\mathrm{PGL}_{2,k}$ a dimension 3 et que l'algèbre de Lie de α_p^n a dimension n. Le résultat que nous montrons est le suivant :

Théorème 3. *Soit k un corps de caractéristique 2.*

1. *Les sous-schémas en groupes infinitésimaux unipotents de $\mathrm{PGL}_{2,k}$ sont exactement, à isomorphisme près, les sous-schémas en groupes du produit semi-direct $\alpha_{2^n,k} \rtimes \alpha_{2,k}$, avec $n \geq 1$, où l'action de $\alpha_{2,k}$ sur $\alpha_{2^n,k}$ est donnée par $a \cdot b = b + ab^2$*

2. *Si k est parfait, tout sous-schéma en groupes infinitésimal trigonalisable, non unipotent, de $\mathrm{PGL}_{2,k}$ est isomorphe à $\mu_{2^l,k}$ ou au produit semi-direct de $\mu_{2^l,k}$, pour un certain $l \geq 1$, par l'un des deux schémas en groupes unipotents*

(a) *le produit semi-direct* $\alpha_{2^n,k} \rtimes \alpha_2$, *avec* ≥ 1, *où l'action de* $\alpha_{2,k}$ *sur* $\alpha_{2^n,k}$ *est donnée par* $a \cdot b = b + ab^2$.

(b) $\alpha_{2^n,k}$

pour une action non-triviale de $\mu_{2^l,k}$.

Une description explicite de tous ces schémas en groupes sera donnée. Alors que le théorème ci-dessus donne une classification complète des sous-schémas en groupes infinitésimaux unipotents de $\mathrm{PGL}_{2,k}$, pour les schémas en groupes trigonalisables nous ne savons pas si, pour toute action non-triviale de $\mu_{2^l,k}$ sur les schémas en groupes unipotents apparaissant en (a), le produit semi-direct associé agit fidèlement sur $\mathbb{P}^1_k$. Nous prouvons qu'il existe au moins une action de $\mu_{2^l,k}$ sur tout schéma en groupes unipotent qui apparaît dans (a) de telle sorte que le produit semi-direct associé agisse fidèlement sur $\mathbb{P}^1_k$. Dans le cas commutatif et sur un corps algébriquement clos, on obtient la classification complète suivante :

Corollaire. *Soit* k *un corps algébriquement clos de caractéristique* 2. *La liste des sous-schémas en groupes commutatifs infinitésimaux de* $\mathrm{PGL}_{2,k}$, *à isomorphisme près, est la suivante :*

1. $\alpha_{2^n,k}$, *pour* $n \geq 0$,
2. $\alpha_{2,k} \times_k \alpha_{2,k}$,
3. *la* 2*-torsion d'une courbe elliptique supersingulière,*
4. μ_{2^n}, *pour* $n > 0$.

Dans [Kno95] Knop a classifié les sous-schémas en groupes de $\mathrm{SL}_{2,k}$. Bien sûr, il serait possible d'en déduire nos résultats en calculant le quotient de tous les sous-schémas en groupes infinitésimaux trigonalisables de $\mathrm{SL}_{2,k}$. En fait, dans notre approche, il suffit de connaître les sous-schémas en groupes infinitésimaux unipotents de $\mathrm{SL}_{2,k}$, ce qui est beaucoup plus facile.

Il y existe un lien entre ce travail et la notion de dimension essentielle. De manière informelle, la *dimension essentielle* d'un objet algébrique est un entier qui mesure sa complexité. Cette notion a été introduite par Buhler et Reichstein dans [BR97] pour les groupes finis et a ensuite été étendue par Merkurjev pour les foncteurs de la catégorie des extensions de corps d'un corps de base fixé k vers la catégorie des ensembles [BF03].

Pour un k-schéma en groupes G, sa dimension essentielle $\mathrm{ed}_k(G)$ calcule, en gros, le nombre de paramètres nécessaires pour définir tous les G-torseurs sur tous les schémas sur k. Tossici a conjecturé que si k est un corps de caractéristique positive et G un k-schéma en groupes fini commutatif unipotent, alors $\mathrm{ed}_k(G) \geq n_V(G)$ où $n_V(G)$ est l'ordre de nilpotence du morphisme de décalage de G [Tos19, Conjecture 1.4]. On sait que cette conjecture est vraie pour $n_V(G) = 2$ d'après Fakhruddin [Fak20, Théorème 1.1]. L'espoir est que les résultats de cette thèse permettront de progresser dans la démonstration de cette conjecture dans le cas infinitésimal.

Dans l'appendice de ce travail, nous nous concentrons sur l'algèbre du smash-produit, un objet non-commutatif intéressant qui apparaît naturellement lors de l'étude des actions des schémas en groupes commutatifs finis. Un exemple de smash-produit est donné par l'algèbre des polynômes d'Ore $K[X;\theta,\partial]$ où θ est un automorphisme du corps K, ∂ est une θ-dérivation ($\partial(ab) = \theta(a)\partial(b) + \partial(a)b$ pour tout $a, b \in K$) et la loi de multiplication est donnée par $Xa = \theta(a)X + \partial(a)$ pour tout $a \in K$.

La motivation principale pour le contenu de l'appendice provient de notre intérêt à pouvoir faire des calculs avec des dérivations et des opérateurs différentiels, ce qui est nécessaire lorsqu'on traite des actions de schémas en groupes infinitésimaux commutatifs unipotents. Il s'avère que faire des calculs de ce type est équivalent à les faire dans une algèbre de smash-produit définie de manière appropriée. L'utilisation du formalisme des smash-produits s'est avérée très utile pour mieux comprendre et avoir des intuitions à ce niveau.

Les smash-produits ont également un lien avec la théorie du codage. Les polynômes d'Ore y trouvent des applications importantes et sont utilisés pour construire les codes de Gabidulin [Gab85] et les codes de Reed-Solomon linéarisés [Mar18]. Ces deux familles de codes sont la contrepartie, respectivement dans la *rank metric* et dans la *sum-rank metric*, des codes de Reed-Solomon [RS60], qui sont l'une des familles de codes linéaires les plus utilisées dans la métrique de Hamming (centrale depuis les années 50 dans la théorie de la correction d'erreurs). Les codes dans la rank metric ont été introduits pour la première fois par Delsarte [Del78], tandis que ceux dans la sum-rank metric sont de définition plus récente (une référence pour la théorie des codes en sum-rank metric est [MSK22]).

Les codes en géométrie algébrique, une généralisation des codes de Reed-Solomon, ont été introduits par Goppa [Gop82] et sont construits en évaluant les espaces de fonctions en des points rationnels sur des courbes algébriques. Dans [BC23] Berardini et Caruso définissent les codes en géométrie algébrique linéarisés, la première construction géométrique de codes dans la sum-rank metric à partir de courbes algébriques. Leur définition est obtenue en considérant des torseurs sous le k-schéma en groupes commutatif constant fini $G = \mathbb{Z}/r\mathbb{Z}$. Des constructions similaires peuvent être réalisées pour les torseurs sous n'importe quel k-schéma en groupes commutatif fini. Ceci pourrait nous fournir un plus grande collection de codes en géométrie algébrique linéarisés.

Les principaux résultats contenus dans l'appendice concernent l'étude des endomorphismes de certaines algèbres de smash-produits, ainsi qu'une généralisation des résultats de Chase et Sweedler [CS69, Theorems 9.3] et Gamst et Hoechsmann [GH69] autour des smash-produits qui sont des algèbres d'Azumaya.

Contents

Introduction

This thesis focuses on the study of (rational) actions of infinitesimal group schemes, with a particular emphasis on infinitesimal commutative unipotent group schemes and generically free actions and faithful actions. These group schemes exist only in positive characteristic and examples arise looking at the p-torsion of abelian varieties.

The interest in this topic has multiple motivations that we will explain in this introduction. Let k be a field and X be a k-scheme. The automorphism group functor Aut_X of X that associates to every k-scheme S the group of S-automorphisms $\mathrm{Aut}_S(X \times_k S)$ is not representable in general. This object has been extensively studied: it is known for example that if X is proper then Aut_X is represented by a k-group scheme locally of finite type [MO67]. If K/k is a finite purely inseparable field extension, the automorphism group scheme $\mathrm{Aut}_K := \mathrm{Aut}_{\mathrm{Spec}(K)}$ has been studied for example by [Beg69] and [Cha72].

For G a k-group scheme, there is a bijection between G-actions $G \times_k X \to X$ on X and group functor homomorphisms $G \to \mathrm{Aut}_X$. If the G-action is faithful, then G is a subgroup functor of Aut_X. Studying faithful group scheme actions yields then information on representable subgroups of Aut_X. When Y is the generic point of a variety X (separated, geometrically integral scheme of finite type) and G is a finite k-group scheme, to give a G-action on $Y = \mathrm{Spec}(k(X))$ is equivalent to giving a rational G-action on X. Studying such faithful rational actions imparts then knowledge on the automorphism group functor Aut_K of separable finitely generated extensions K/k.

When $K = k(t_1, \ldots, t_n)$ is a purely transcendental extension of k, then $\mathrm{Aut}_K(k)$ coincides with the Cremona group $\mathrm{Cr}_n(k) = \mathrm{Bir}_k(\mathbb{P}^n_k)$ in dimension n, that is by definition the group of birational automorphisms of $\mathbb{P}^n_k$. The Cremona group has been deeply studied in characteristic zero, while it has been less investigated in positive characteristic (see for example the survey [Dol10]). Dolgachev made the following conjecture for the Cremona group over a field of positive characteristic.

Conjecture. If k is a field of characteristic $p > 0$, the Cremona group $\mathrm{Cr}_n(k)$ does not contain elements of order p^s for $s > n$ [Dol10, Conjecture 37].

The conjecture is true for $n = 1$ since $\mathrm{PGL}_2(k) \simeq \mathrm{Aut}_k(k(t))$ does not contain elements of order p^2 if $char(k) = p > 0$. Moreover, it was proven for $n = 2$ [Dol09]. The conjecture can be rephrased in the following way: if there exists a faithful rational action of a finite commutative p-group G on $\mathbb{P}^n_k$ then $p_G^n = 0$, where p_G is the multiplication by p morphism on G. Indeed there is a natural correspondence between faithful actions

of a finite commutative p-group G on $k(t_1, \dots, t_n)$ and faithful rational actions of the corresponding constant group scheme on $\mathbb{P}^n_k$.

In this thesis we are interested in rational actions of infinitesimal group schemes. The analogous of Dolgachev's conjecture for infinitesimal commutative unipotent group schemes arises naturally in one of the following ways: if k is a field of characteristic $p > 0$ and G is an infinitesimal commutative unipotent k-group scheme, if there exists a faithful rational G-action on $\mathbb{P}^n_k$, then $p^n_G = 0$ (or maybe $V^n_G = 0$, where V_G is the Verschiebung morphism of G). Both options turn out not to be true. Indeed, for example any curve admits faithful rational actions of the p^n-torsion $E[p^n]$ of a supersingular elliptic curve E (since in this case $E[p^n]$ is an infinitesimal commutative unipotent k-group scheme with one-dimensional Lie algebra and thus Theorem 3.2.13 applies) but $V_{E[p^n]} \neq 0$, and $p_{E[p^n]} \neq 0$ if $n > 1$.

What is indeed true is that if there exists a faithful rational G-action on a k-variety X of dimension n, then $V^n_{\ker(F_G)} = 0$. More precisely:

Proposition 3.3.6. *Let G be an algebraic k-group scheme with commutative Frobenius kernel and X be a k-variety of dimension n. If there exists a faithful rational G-action on X, then $s = dim_k(\mathrm{Lie}(\ker(F_G)^m)) \leq n$ and $V^{n-s}_{\ker(F_G)^u} = 0$, where $\ker(F_G)^m$ is the maximal k-subgroup scheme of multiplicative type of $\ker(F_G)$ and $\ker(F_G)^u := \ker(F_G)/\ker(F_G)^m$.*

We give a proof of this result in Section 3.3 of Chapter 3. The inverse implication of Proposition 3.3.6 does not always hold true, see Example 3.3.7. In the diagonalizable case, these actions are well understood and the converse statement is known. Moreover, we show that there exist faithful rational actions of any infinitesimal commutative unipotent group scheme G defined over a perfect field on any variety of dimension n if $V^n_G = 0$ (Proposition 3.3.10). As a consequence, the converse of Proposition 3.3.6 holds true over a perfect field for infinitesimal commutative unipotent k-group schemes of height one.

We are more precisely interested in rational actions which are generically free. Indeed in positive characteristic not all faithful actions admit an open dense subset $U \subseteq X$ that is G-stable and such that the action of G on U is free. For any finite k-group scheme G acting rationally on a k-variety X, if the action is generically free then the dimension of $\mathrm{Lie}(G)$ is upper bounded by the dimension of the variety. One of the main results of this thesis is the following Theorem, which proves that this bound is the only obstruction to the existence of generically free rational actions for infinitesimal commutative trigonalizable group schemes over a perfect field (see Remark 3.2.14). If G is unipotent, we also show that any generically free rational action on X of (any power of) the Frobenius kernel of G extends to a generically free rational action of G on X. The proof we give is constructive and enables one to explicitly write such actions: we end Section 3.2 of Chapter 3 with several examples showing it concretely.

Theorem 3.2.13. *Let k be a perfect field of characteristic $p > 0$ and G be an infinitesimal commutative unipotent k-group scheme with Lie algebra of dimension s. Then for every k-variety X of dimension $\geq s$ there exist generically free rational actions of G on X. Moreover, for any $r \geq 1$, any generically free rational action of $\ker(F^r_G)$ on X can be extended to a generically free rational action of G on X.*

The difficulty is to construct actions in low dimension, i.e. close to the dimension of $\mathrm{Lie}(G)$. Indeed, it is not so difficult to construct actions in high dimension for any infinitesimal trigonalizable group scheme (see Corollary 3.2.6). Combining Theorem 3.2.13 and the diagonalizable case treated by Brion in [Bri22, Section 3] the converse of Proposition 3.3.6 is true, over a perfect field, for infinitesimal commutative trigonalizable k-group schemes with Lie algebra of dimension upper bounded by the dimension of the variety (in particular, if $s = \dim_k(\mathrm{Lie}(\ker(F_G)^d))$ and $\dim_k(\mathrm{Lie}(G)) \leq n$, then $V^{n-s}_{\ker(F_G)^u} = 0$).

Notice that if an infinitesimal commutative unipotent k-group scheme G with Lie algebra of dimension n can be embedded in a smooth connected n-dimensional algebraic group $\mathcal{G}$, then G acts generically freely on it (by multiplication). Brion asked [Bri22] if, already in the one-dimensional case, there are examples different from these that arise and moreover if these group schemes are always commutative (see also [Fak20, Remark 2.10]). Proposition 2.3.12 and Example 2.3.13 combined with Theorem 3.2.13 answer to these questions. The former shows that there are generically free rational actions on curves of infinitesimal commutative unipotent group schemes that are not subgroups of a smooth connected one-dimensional algebraic group. The latter shows that there exist generically free rational actions of non-commutative infinitesimal group schemes on varieties.

In general, it is not easy to describe explicitly infinitesimal commutative unipotent group schemes. For example, already those arising as the p-torsion of some abelian variety (with p-rank zero) are not completely understood and increase in complexity as the dimension grows. To have an explicit description of such group schemes, for example in terms of the Hopf algebra representing them, is useful in order to construct actions of these group schemes on varieties (see for example Proposition 3.1.17). The following result gives an explicit description of all infinitesimal commutative unipotent k-group schemes with one-dimensional Lie algebra defined over an algebraically closed field k, answering partially to a question of Fakhruddin (see [Fak20, Remark 2.10]).

Theorem 2.3.1. *Let k be an algebraically closed field of characteristic $p > 0$. For any $n \geq 1$, there are exactly, up to isomorphism, n infinitesimal commutative unipotent k-group schemes of order p^n and with one-dimensional Lie algebra. They are the group schemes of the form*

$$W_n^n[V - F^i] := \ker(V - F^i \colon W_n^n \to W_n^n)$$

for some $i = 1, \ldots, n$.

This result is known for infinitesimal commutative unipotent group schemes of order $\leq p^3$ thanks to [Oor66, (15.5)] and [NWW15, Theorem 1.1].

Of these group schemes, the only ones that are contained in a smooth connected algebraic group are α_{p^n} and $W_n^n[F - V]$ (the former is a subgroup of $\mathbb{G}_a$ and the latter is contained in the p^n-torsion of a supersingular elliptic curve) for any $n \geq 1$, see Proposition 2.3.12. All the others are examples of infinitesimal group schemes that act generically freely on any curve (by Theorem 3.2.13), but are not subgroups of a smooth connected one-dimensional algebraic group. Notice moreover that $W_n^n[F - V]$ is the only self-dual

group scheme of the list. If one considers infinitesimal commutative unipotent group schemes with higher dimensional Lie algebra, this is not the case anymore: indeed the p-torsion of any principally polarized abelian variety of dimension g and p-rank zero, is an infinitesimal commutative unipotent group scheme, and there exist p^{g-1} different isomorphism classes of such varieties (see [Pri08]).

Fakhruddin proved that if G is infinitesimal and Y is a normal projective curve with a rational action of G, if there exists a normal projective variety X with an action of G and a G-equivariant dominant rational morphism $X \dashrightarrow Y$, then the rational action of G on Y extends uniquely to an action of G on Y [Fak20, Proposition 2.2]. In particular, in the above situation, if Y is the projective line and the action is faithful, then G is a subgroup scheme of $\mathrm{PGL}_{2,k}$. Most unipotent infinitesimal group schemes with one-dimensional Lie algebra are not contained in $\mathrm{PGL}_{2,k}$, but for all of them there exist generically free rational actions on the projective line. Therefore, most of these rational actions on the projective line are not induced by actions, defined everywhere, on projective normal varieties of higher dimension.

If the characteristic of a field k is odd, any infinitesimal subgroup scheme of $\mathrm{PGL}_{2,k}$ lifts to $\mathrm{SL}_{2,k}$. In the last section of Chapter 3, whose content comes entirely from [GT24], we prove that this is not true in characteristic 2 and we give a complete description, up to isomorphism, of infinitesimal unipotent subgroup schemes of $\mathrm{PGL}_{2,k}$. Also, the infinitesimal trigonalizable case is considered.

In his paper [Bea10], Beauville classified, up to conjugacy, all finite subgroups of $\mathrm{PGL}_2(k)$ of order coprime with the characteristic. Here we are interested in the opposite case, infinitesimal subgroup schemes. It seems that it is quite an accepted fact that any infinitesimal subgroup scheme of $\mathrm{PGL}_{2,k}$ lifts to $\mathrm{GL}_{2,k}$. In particular any unipotent infinitesimal subgroup scheme of $\mathrm{PGL}_{2,k}$ would be a subgroup scheme of $\mathbb{G}_{a,k}$, and so it would be isomorphic to $\alpha_{p^n,k}$ for some $n \geq 0$. We prove that this is not true if the characteristic of the field is 2. The result is instead true if the characteristic is odd and we give a proof of it (see Proposition 3.4.4).

For any field k, $\mathrm{PGL}_{2,k}$ represents the automorphism group functor of $\mathbb{P}^1_k$. So the study of subgroup schemes corresponds to faithful actions on $\mathbb{P}^1_k$. Moreover $\mathrm{PGL}_{2,k}(k)$ coincides with the Cremona group in dimension one, i.e. birational self-maps of $\mathbb{P}^1_k$, since any rational self-map from a projective nonsingular curve extends to the whole curve. In positive characteristic, the situation is completely different if we consider rational actions of infinitesimal group schemes. Most of the faithful infinitesimal actions on the affine line do not extend to $\mathbb{P}^1_k$. For instance, all the faithful actions of α_p^n, with $n \geq 4$, on $\mathbb{A}^1_k$ do not extend to $\mathbb{P}^1_k$, since $\mathrm{PGL}_{2,k}$ has dimension 3 and the Lie algebra of α_p^n has dimension n. The main result of this section is the following.

Theorem 3.4.1. *Let k be a field of characteristic 2.*

1. *The infinitesimal unipotent subgroup schemes of $\mathrm{PGL}_{2,k}$ are exactly, up to isomorphism, the subgroup schemes of the semi-direct product $\alpha_{2^n,k} \rtimes \alpha_{2,k}$, with $n \geq 1$, where the action of $\alpha_{2,k}$ on $\alpha_{2^n,k}$ is given by $s \cdot t = t + st^2$.*

2. *If k is perfect, any infinitesimal trigonalizable, not unipotent, subgroup scheme of*

$\mathrm{PGL}_{2,k}$ *is isomorphic to* $\mu_{2^l,k}$ *or to the semi-direct product of* $\mu_{2^l,k}$*, for some* $l \geq 1$*, by one of the two unipotent group schemes*

(a) the semi-direct product $\alpha_{2^n,k} \rtimes \alpha_2$*, with* $n \geq 1$*, where the action of* $\alpha_{2,k}$ *on* $\alpha_{2^n,k}$ *is given by* $s \cdot t = t + st^2$

(b) $\alpha_{2^n,k}$

for some non-trivial action of $\mu_{2^l,k}$*.*

An explicit description of all these group schemes will be given. While the above Theorem gives a complete classification of infinitesimal unipotent subgroup schemes of $\mathrm{PGL}_{2,k}$, for trigonalizable group schemes we do not know if, for any non-trivial action of $\mu_{2^l,k}$ over the unipotent group schemes in (a), the associated semi-direct product acts faithfully on $\mathbb{P}^1_k$. We prove that there exists at least one action of $\mu_{2^l,k}$ over any unipotent group scheme which appears in (a) such that the associated semi-direct product acts faithfully on $\mathbb{P}^1_k$. In the commutative case, we get a complete classification over an algebraically closed field.

Corollary 3.4.2. *Let* k *be an algebraically closed field of characteristic* 2*. The list of infinitesimal commutative subgroup schemes of* $\mathrm{PGL}_{2,k}$*, up to isomorphism, is the following:*

1. $\alpha_{2^n,k}$*, for some* $n \geq 0$*,*
2. $\alpha_{2,k} \times \alpha_{2,k}$*,*
3. *the* 2*-torsion of a supersingular elliptic curve,*
4. μ_{2^n}*, for some* $n > 0$*.*

The Corollary follows from Theorem 3.4.1 using Lemma 3.4.7. In [Kno95] Knop classified subgroup schemes of $\mathrm{SL}_{2,k}$. Of course, it could be possible to deduce our results by computing the quotient of all infinitesimal trigonalizable subgroup schemes of $\mathrm{SL}_{2,k}$. In fact, in our approach, we just need to know infinitesimal unipotent subgroup schemes of $\mathrm{SL}_{2,k}$, which is much easier.

Let us spend also a few words on the existing link between this work and the notion of essential dimension. Informally speaking, the *essential dimension* of an algebraic object is an integer that measures its complexity. This notion was introduced by Buhler and Reichstein in [BR97] for finite groups and was then extended by Merkurjev for functors from the category of field extensions of a fixed base field k to the category of sets [BF03].

For a k-group scheme G, its essential dimension $\mathrm{ed}_k(G)$ computes, roughly speaking, the number of parameters needed to define all G-torsors over all schemes over k. Tossici conjectured that if k is a field of positive characteristic and G is a finite commutative unipotent k-group scheme, then $\mathrm{ed}_k(G) \geq n_V(G)$ where $n_V(G)$ is the order of nilpotency of the Verschiebung morphism of G [Tos19, Conjecture 1.4]. The conjecture is known to be true for $n_V(G) = 2$ after Fakhruddin [Fak20, Theorem 1.1]. Our hopes are that

Theorem 3.2.13 might lead to further progress in the proof of this conjecture in the infinitesimal case.

In the appendix of this work we focus on the smash product algebra, an interesting non-commutative object that arises naturally when studying actions of finite commutative group schemes. An example of smash product is given by the algebra of Ore polynomials $K[X;\theta,\partial]$ where θ is an automorphism of the field K, ∂ is a θ-derivation ($\partial(ab) = \theta(a)\partial(b)+\partial(a)b$ for all $a,b \in K$) and the multiplication law is given by $Xa = \theta(a)X+\partial(a)$ for any $a \in K$.

The main motivation for the content of the appendix arises from our interest in being able to do computations with derivations and differential operators, something that is necessary when dealing with actions of infinitesimal commutative unipotent group schemes. It turns out that doing computations of this kind is equivalent to doing them in an appropriately defined smash-product algebra. Using the formalism of smash-products proved itself of great help in order to have a better understanding and having intuitions at this level.

Smash-products have also a tight link to coding theory. Ore polynomials have important applications in it and are used to construct Gabidulin [Gab85] and linearised Reed-Solomon codes [Mar18]. These two families of codes are the counterpart respectively in the rank metric and in the sum-rank metric of Reed-Solomon codes [RS60], which form one of the most used families of linear codes in the Hamming metric (central since the 50's in the theory of error correction). Codes in the rank metric where first introduced by Delsarte [Del78], while those in the sum-rank metric are of more recent definition (a reference for the theory of sum-rank metric codes is [MSK22]).

Algebraic Geometry codes, a generalization of Reed-Solomon codes, were introduced by Goppa [Gop82] and are constructed by evaluating spaces of functions at rational points on algebraic curves. In [BC23] Berardini and Caruso define Linearised Algebraic Geometry codes, the first geometric construction of codes in the sum-rank metric from algebraic curves. Their definition arises from considering torsors under the finite constant commutative k-group scheme $G = \mathbb{Z}/r\mathbb{Z}$. Similar constructions can be done for torsors under any finite commutative k-group scheme. Doing this could provide us with a larger panel of linearized Algebraic Geometry codes.

The main results contained in the appendix involve the study of the endomorphisms of certain smash-product algebras (see Proposition A.1.4), along with a generalization of results of Chase and Sweedler [CS69, Theorems 9.3] and Gamst and Hoechsmann [GH69] around smash-products being Azumaya algebras (see Proposition A.2.11).

A consistent part of the contents of this thesis appears already in the papers [Gou23] and [GT24] (joint with Dajano Tossici): more precisely the results appearing in Section 1.2 of Chapter 1, Section 2.2 of Chapter 2 and Sections 3.2 and 3.3 of Chapter 3 are the content of the first cited paper, while the second cited paper is presented in Section 3.4.

Outline

Here is an outline of the contents of this work.

In Chapter 1 we begin by recalling the definitions of some basic algebraic structures, ending with the definition of a Hopf algebra. We then move to (co)-module algebras and smash products, objects that have a tight link with actions of group schemes (see Proposition 3.1.17). In the second section of this chapter we deal with nilpotent derivations, which are often encountered when studying actions of infinitesimal group schemes (see Proposition 3.1.18 and Example 3.1.19). Moreover, we study p-bases of finite field extensions and we prove Corollary 1.2.7 describing when some systems of differential equations admit a solution. This result plays an important role in the proof of Theorem 3.2.13.

In Chapter 2 we start by recalling some notions and results around finite (commutative) group schemes, with a strong emphasis on infinitesimal commutative unipotent group schemes. We also introduce the *socle* of a finite group scheme, an object which proves itself helpful when studying generically free or faithful actions of a finite group scheme (see for example Proposition 3.2.1 and Proposition 3.3.1). Moreover, we prove Proposition 2.2.30 giving a description of the Hopf algebra of an infinitesimal commutative unipotent group scheme over a perfect field. This result is another of the building blocks needed for the proof of Theorem 3.2.13. The last section is devoted to proving Theorem 2.3.1, which describes explicitly all infinitesimal commutative unipotent group schemes with one-dimensional Lie algebra over an algebraically closed field k.

The first section of Chapter 3 is devoted to generalities on (rational) actions of finite group schemes on varieties and their algebraic counterpart given by module algebra structures, introduced already in Chapter 1. In Section 3.2 we deal with generically free actions. In the first part we prove the existence part of Theorem 3.2.13 in the case of commutative trigonalizable group schemes of height one (Proposition 3.2.4). We then proceed with the proof of the general case. We end the section with some examples to show more concretely how to deal with the construction of these actions.

Section 3.3 is devoted to Dolgachev's conjecture revisited for infinitesimal group schemes and, more generally, to studying faithful rational actions of infinitesimal group schemes. Proposition 3.3.6 gives necessary (but not sufficient, see the counterexample 3.3.7) conditions for the existence of faithful rational actions of infinitesimal commutative trigonalizable group schemes. Moreover, we show that there exist faithful rational actions of any infinitesimal commutative unipotent group scheme G defined over a perfect field on any variety of dimension n if $V_G^n = 0$ (Proposition 3.3.10). We illustrate our results about faithful rational actions in the case of the connected part of the p-torsion of abelian varieties.

Section 3.4 has as content the work [GT24], joint with Dajano Tossici, where unexpected subgroup schemes of $\mathrm{PGL}_{2,k}$ in characteristic 2 are studied. If the characteristic of a field k is odd any infinitesimal group scheme of $\mathrm{PGL}_{2,k}$ lifts to $\mathrm{SL}_{2,k}$. We prove that this is not true in characteristic 2 and we give a complete description, up to isomorphism, of infinitesimal unipotent subgroup schemes of $\mathrm{PGL}_{2,k}$. Also, the infinitesimal trigonalizable

case is considered.

Appendix A contains a deeper study of smash-products. In the first section we study the endomorphisms of the smash-product algebra. In Section A.2, inspired by the results of Chase and Sweedler [CS69, Theorems 9.3] and Gamst and Hoechsmann [GH69], we give a generalization around smash-products being Azumaya algebras (see Proposition A.2.11). In Section A.3 we introduce a universal object that allows us to doing computations in a universal smash-product algebra, helping us at simplify and have insights on computations involving derivations and differential operators (which was our main motivation for investigating smash-product). In the last section of the appendix we revisit some results already known in literature, and that we recover and generalize also in the previous section, around the reduced norm of some Ore polynomials, giving also alternative proofs.

Chapter 1

Hopf algebras and nilpotent derivations

In the first part of this chapter we recall the definitions of some basic algebraic structures, ending with the definition of a Hopf algebra. These objects are interesting on their own but they moreover occupy a central role in the theory of group schemes since any affine group scheme is encoded by a commutative Hopf algebra. We then move to (co)-module algebras and smash products, which have a tight link with actions of group schemes (see Proposition 3.1.17) and thus play a key part in this work. The second section of this chapter is devoted to nilpotent derivations, which are often encountered when studying actions of infinitesimal group schemes (see Proposition 3.1.18 and Example 3.1.19). Proposition 1.2.6 and Corollary 1.2.7 will play an important role in the proof of Theorem 3.2.13, which is one of the main results of this work.

1.1 Algebraic structures

Some references for this section are [Swe69, Chapter VII] and [Mon93, Chapter 4].

Algebras, coalgebras and Hopf algebras

Let R be a commutative ring.

Definition 1.1.1 (Algebra)**.** An *R-algebra* is a triple (A, m, u) where A is an R-module and $m\colon A \otimes_R A \to A$ (multiplication) and $u\colon R \to A$ (unit) are R-linear morphisms such that the following diagrams commute:

$$\begin{array}{ccc} A \otimes_R A \otimes_R A & \xrightarrow{m\otimes 1} & A \otimes_R A \\ \downarrow{\scriptstyle 1\otimes m} & & \downarrow{\scriptstyle m} \\ A \otimes_R A & \xrightarrow{\quad m \quad} & A, \end{array} \qquad \begin{array}{ccccc} & & A \otimes_R A & & \\ & \nearrow^{u\otimes 1} & \downarrow{\scriptstyle m} & \nwarrow_{1\otimes u} & \\ R \otimes_R A & & & & A \otimes_R R \\ & \searrow & & \swarrow & \\ & & A. & & \end{array}$$

Notice that the first diagram tells us that the multiplication m is associative but we don't ask (a priori) for it to be commutative and that the second diagram tells us in particular that the image of R in A is contained in its center ($u(R) \subseteq Z(A)$). An R-algebra A is said to be *commutative* if the following diagram commutes:

$$\begin{array}{ccc} A \otimes_R A & \xrightarrow{\tau} & A \otimes_R A \\ & {\scriptstyle m}\searrow \quad \downarrow{\scriptstyle m} & \\ & A & \end{array}$$

where we denote by τ the switch morphism, $\tau\colon x \otimes y \mapsto y \otimes x$ for any $x, y \in A$.

Definition 1.1.2 (Coalgebra)**.** An *R-coalgebra* is a triple (C, Δ, ε) where A is an R-module and $\Delta\colon C \to C \otimes_R C$ (comultiplication) and $\varepsilon\colon C \to R$ (counit) are R-linear morphisms such that the following diagrams commute:

$$\begin{array}{ccc} C \otimes_R C \otimes_R C & \xleftarrow[\Delta\otimes 1]{} & C \otimes_R C \\ {\scriptstyle 1\otimes\Delta}\uparrow & & \uparrow{\scriptstyle \Delta} \\ C \otimes_R C & \xleftarrow[\Delta]{} & C, \end{array} \qquad \begin{array}{ccccc} & & C \otimes_R C & & \\ & {\scriptstyle \varepsilon\otimes 1}\swarrow & \uparrow{\scriptstyle \Delta} & \searrow{\scriptstyle 1\otimes\varepsilon} & \\ R \otimes_R C & & & & C \otimes_R R \\ & \nwarrow & \uparrow & \nearrow & \\ & & C. & & \end{array}$$

Notice that the first diagram tells us that the comultiplication Δ is coassociative but we don't ask (a priori) for it to be cocommutative. An R-coalgebra C is said to be *cocommutative* if the following diagram commutes:

$$\begin{array}{ccc} C \otimes_R C & \xleftarrow{\tau} & C \otimes_R C \\ & {\scriptstyle \Delta}\nwarrow \quad \uparrow{\scriptstyle \Delta} & \\ & C & \end{array}$$

where τ is the switch morphism.

Definition 1.1.3 (Coideal)**.** Let C be an R-coalgebra. A *coideal* is an R-submodule I of C such that:

1. $\Delta(I) \subseteq I \otimes_R C + C \otimes_R I$;
2. $\varepsilon(I) = 0$.

Definition 1.1.4 (Primitive element)**.** Let C be an R-coalgebra. An element $x \in C$ is *primitive* if $\Delta(x) = x \otimes 1 + 1 \otimes x$.

Remark 1.1.5.

(i) For any primitive element x of an R-coalgebra C it holds $\varepsilon(x) = 0$.

(ii) Let A and B be R-algebras, then $A \otimes_R B$ is an R-algebra with multiplication

$$m_{A\otimes_R B} \colon (A \otimes_R B) \otimes_R (A \otimes_R B) \xrightarrow{\mathrm{id}\otimes\tau\otimes\mathrm{id}} A \otimes_R A \otimes_R B \otimes_R B \xrightarrow{m_A\otimes m_B} A \otimes_R B$$

(where τ is the switch morphism) and unit

$$u_{A\otimes_R B} \colon R \simeq R \otimes_R R \xrightarrow{u_A\otimes u_B} A \otimes_R B.$$

(iii) Let C and D be R-coalgebras, then $C \otimes_R D$ is an R-coalgebra with comultiplication

$$\Delta_{C\otimes_R D} \colon C \otimes_R D \xrightarrow{\Delta_C\otimes\Delta_D} C \otimes_R C \otimes_R D \otimes_R D \xrightarrow{\mathrm{id}\otimes\tau\otimes\mathrm{id}} (C \otimes_R D) \otimes_R (C \otimes_R D)$$

and counit

$$\varepsilon_{C\otimes_R D} \colon C \otimes_R D \xrightarrow{\varepsilon_C\otimes\varepsilon_D} R \otimes_R R \simeq R.$$

(iv) Let (A, m, u) be an R-algebra and (C, Δ, ε) be an R-coalgebra. Then $\mathrm{Hom}_R(C, A)$ is an R-algebra where multiplication and unit are respectively given by

$$f \otimes g \mapsto f * g := m \circ (f \otimes g) \circ \Delta, \quad \text{and} \quad u \circ \varepsilon.$$

The multiplication of this algebra is often referred to as *convolution product*. Notice that the associativity of the convolution product follows from the associativity of m and the coassociativity of Δ.

Definition 1.1.6 (Bialgebra)**.** An *R-bialgebra* is a tuple $(H, m, u, \Delta, \varepsilon)$ such that

1. (H, m, u) is an R-algebra;
2. (H, Δ, ε) is an R-coalgebra;
3. one of the following equivalent conditions holds true:
   (a) m and u are morphisms of coalgebras;
   (b) Δ and ε are morphisms of algebras;
   (c) the following diagrams commute:

$$\begin{array}{ccccc}
H \otimes_R H & \xrightarrow{\quad m \quad} & H & \xrightarrow{\quad \Delta \quad} & H \otimes_R H \\
\downarrow{\scriptstyle \Delta\otimes\Delta} & & & & \uparrow{\scriptstyle m\otimes m} \\
H \otimes_R H \otimes_R H \otimes_R H & & \xrightarrow{\quad \mathrm{id}\otimes\tau\otimes\mathrm{id} \quad} & & H \otimes_R H \otimes_R H \otimes_R H,
\end{array}$$

$$\begin{array}{ccc}
H \otimes_R H & \xrightarrow{\quad \varepsilon\otimes\varepsilon \quad} & R \otimes_R R \\
\downarrow{\scriptstyle m} & & \downarrow \\
H & \xrightarrow{\quad \varepsilon \quad} & R,
\end{array}$$

$$\begin{array}{ccc} H & \xrightarrow{\Delta} & H \otimes_R H \\ {\scriptstyle u}\uparrow & & \uparrow{\scriptstyle u\otimes u} \\ R & \longrightarrow & R \otimes_R R, \end{array} \qquad \begin{array}{ccc} & H & \\ {\scriptstyle \varepsilon}\swarrow & & \nwarrow{\scriptstyle u} \\ R & \longrightarrow & R. \end{array}$$

Notice that the commutativity of the first and second diagram tells that m is a morphism of coalgebras (recall that $m_{H\otimes_R H} = m \otimes m \circ (\mathrm{id} \otimes \tau \otimes \mathrm{id})$), the commutativity of the first and third that Δ is a morphism of algebras (recall that $\Delta_{H\otimes_R H} = (\mathrm{id} \otimes \tau \otimes \mathrm{id}) \circ \Delta \otimes \Delta$), the commutativity of the second and fourth tells that ε is a morphism of algebras and the commutativity of the third and fourth tells that u is a morphism of coalgebras and that Δ is unitary.

Example 1.1.7. Let k be a field and $(A, m, u, \Delta, \varepsilon)$ be a finite dimensional k-bialgebra, then $A^\vee := \mathrm{Hom}_k(A, k)$ is a finite dimensional k-bialgebra with multiplication and comultiplication respectively given by the convolution product

$$\begin{aligned} m^\vee \colon A^\vee \otimes_k A^\vee &\to A^\vee \\ f \otimes g &\mapsto (A \xrightarrow{\Delta} A \otimes_k A \xrightarrow{f\otimes g} k \otimes_k k \simeq k) \end{aligned}$$

and

$$\begin{aligned} \Delta^\vee \colon A^\vee &\to A^\vee \otimes_k A^\vee \\ \varphi &\mapsto (A \otimes_k A \xrightarrow{m} A \xrightarrow{\varphi} k) \end{aligned}$$

and unit and counit respectively given by the dual morphisms of ε and u.

Definition 1.1.8 (Bi-ideal)**.** Let H be an R-bialgebra. A *bi-ideal* is an R-submodule I of H which is an ideal and a coideal.

Definition 1.1.9 (Antipode)**.** Let H be an R-bialgebra. An *antipode* is an element $S \in \mathrm{Hom}_R(H, H)$ which is a multiplicative (right and left) inverse to the identity, that is $\mathrm{id} * S = S * \mathrm{id} = u \circ \varepsilon$ (where $*$ is the convolution product).

Definition 1.1.10 (Hopf algebra)**.** An *R-Hopf algebra* is a bialgebra which has also an antipode.

Definition 1.1.11 (Hopf ideal)**.** Let H be an R-Hopf algebra. A *Hopf ideal* is a bi-ideal I such that $S(I) \subseteq I$.

Proposition 1.1.12. *There is an anti-equivalence of categories between the category of commutative R-Hopf algebras and the category of affine group schemes over* $\mathrm{Spec}(R)$ *given by assigning any R-Hopf algebra H to* $\mathrm{Spec}(H)$.

Proof. See [Mil17, Chapter 3, Proposition 3.6] □

Module algebras, comodule algebras and smash products

Let R be a commutative ring and A be an R-bialgebra.

Definition 1.1.13 (Module algebra)**.** We say that an R-algebra B is a (left) *A-module algebra* if:

1. B is a (left) A-module via $\psi\colon A \otimes_R B \to B, a \otimes b \mapsto a \cdot b$;
2. the morphism $\eta\colon B \to \mathrm{Hom}_R(A, B), b \mapsto (a \mapsto a \cdot b)$ is a (unital) morphism of R-algebras.

We can give the same definition on the right as well.

The following remark is of key importance for the way in which we will view module algebras throughout this whole work.

Remark 1.1.14. Notice that the first condition of the above definition is equivalent to giving a map

$$v\colon A \to \mathrm{End}_R(B), a \mapsto (b \mapsto a \cdot b)$$

which is a morphism of R-algebras, while the second request corresponds to asking that v satisfies the following properties:

$$\begin{cases} v(a)(1) = \varepsilon(a) \\ v(a)(fg) = m_B(v \otimes v \circ \Delta(a))(f \otimes g) \end{cases} \tag{1.1}$$

for any $a \in A$ and $f, g \in B$. Here ε denotes the counit of A, Δ its comultiplication and m_B the multiplication of B. We will refer to (1.1) as the *property of compatibility with products*. The first statement is straightforward. For the second one, recall that $\mathrm{Hom}_R(A, B)$ has a structure of R-algebra (Remark 1.1.5) with multiplication given by the convolution product

$$\phi \otimes \chi \mapsto m_B \circ \phi \otimes \chi \circ \Delta$$

and unit

$$R \to \mathrm{Hom}_R(C, B), x \mapsto (c \mapsto \varepsilon(c)1_B(x)).$$

Moreover $\eta(b)(a) = v(a)(b)$. Therefore, η is a morphism of (unital) R-algebras if and only if

$$\eta(fg) = m_B \circ \eta(f) \otimes \eta(g) \circ \Delta \quad \text{and} \quad \eta(1) = 1_{\mathrm{Hom}_R(A,B)}$$

for all $f, g \in B$ if and only if

$$v(a)(fg) = \eta(fg)(a) = m_B \circ \eta(f) \otimes \eta(g) \circ \Delta(a) = m_B(v \otimes v \circ \Delta(a))(f \otimes g)$$

and

$$v(a)(1) = \eta(1)(a) = \varepsilon(a)$$

for any $a \in A$. Finally, notice that, if we denote by $I := \ker(\varepsilon)$ the augmentation ideal of A, then by what we just showed it holds $v(a)(1) = 0$ for any $a \in I$.

Example 1.1.15. Let G be a finite group and B be an R-algebra. Consider moreover the group-algebra $R[G]$ on G which is a R-bialgebra if we turn any element of G into a group-like element, that is we define $\Delta(g) = g \otimes g$ and $\varepsilon(g) = 1$ for all $g \in G$ (and extend Δ and ε to morphisms of R-algebras on $R[G]$). There is a one-to-one correspondence between actions of the group G on B and $R[G]$-module algebra structures on B. Indeed, any action $G \to \mathrm{Aut}_{\mathbf{Alg}_R}(B)$ of G on B extends naturally to a morphism of R-algebras $R[G] \to \mathrm{Aut}_{\mathbf{Alg}_R}(B)$ which respects also the property (1.1) by the bialgebra structure on $R[G]$.

Definition 1.1.16 (Morphism of module algebras)**.** Let A and A' be R-bialgebras, $\varphi\colon A \to A'$ be a morphism of algebras and B and B' be respectively an A-module algebra and an A'-module algebra via $\psi\colon A \otimes_R B \to B$ and $\psi'\colon A \otimes_R B' \to B'$. We call *morphism of module algebras (with respect to φ)* a morphism of algebras $f\colon B \to B'$ that respects the module algebra structures, that is the following diagram commutes

$$\begin{array}{ccc} A \otimes_R B & \xrightarrow{\psi} & B \\ \downarrow{\scriptstyle \varphi\otimes f} & & \downarrow{\scriptstyle f} \\ A' \otimes_R B' & \xrightarrow{\psi'} & B'. \end{array}$$

Remark 1.1.17. In the above definition, when B and B' are both A-module algebras, one can take φ to be the identity on A. We then have that a *morphism of A-module algebras* $B \to B'$ is just a morphism of A-algebras.

Remark 1.1.18. Let B be an A-module algebra via $v\colon A \to \mathrm{End}_R(B)$ and consider

$$\ker(v) = \{a \in A \mid a \cdot b = 0 \quad \forall b \in B\}.$$

In general $\ker(v)$ is not a bi-ideal (nevertheless, in the Appendix A we will be interested in the case in which $\ker(v)$ is a Hopf ideal). Take for example $A = R[T]$, the Hopf algebra representing the additive group scheme $\mathbb{G}_a$, that is $\Delta(T) = T \otimes 1 + 1 \otimes T$, with R a ring of positive characteristic $p > 2$, $B = R[X]/(X^{p+1})$ and consider the A-module algebra structure on B given by

$$\begin{aligned} v\colon R[T] &\to \mathrm{End}_R(B) \\ T &\mapsto X^p\partial \end{aligned}$$

where ∂ is a non-zero derivation on B. Then we have $T^2 \in \ker(v)$, in fact $\partial(X^p) = 0$ and $X^{p^2} = 0$ in B and thus $X^p\partial \circ X^p\partial = X^{p^2}\partial^2 = 0$. On the other hand,

$$\Delta(T^2) = T^2 \otimes 1 + 2T \otimes T + 1 \otimes T^2$$

does not lie in $\ker(v) \otimes_R A + A \otimes_R \ker(v)$ since $char(k) \neq 2$.

Definition 1.1.19 (Comodule algebra)**.** We say that an R-algebra C is a (right) *A-comodule algebra* if:

1. C is a (right) A-comodule via $\rho\colon C \to C \otimes_R A$;
2. ρ is a morphism of algebras.

We can give the same definition on the left as well.

If A is a commutative R-Hopf algebra and C is a commutative R-algebra, then saying that C is a (right) A-comodule algebra is equivalent to saying that there is a (right) schematic action of the affine group scheme $\mathrm{Spec}(A)$ on the affine scheme $\mathrm{Spec}(C)$.

Remark 1.1.20.

1. Notice that the second condition of the above definition is equivalent to asking that the multiplication m_C and unit u_C of C are morphisms of (right) A-comodules.
2. When A is finite-dimensional one sees that B is a left A-module algebra if and only if it is a right $A^\vee$-comodule algebra (and the same holds with left and right reversed). If in addition A is a cocommutative Hopf algebra and B is commutative, this is also equivalent to giving a schematic action $\mathrm{Spec}(B) \times_R \mathrm{Spec}(A^\vee) \to \mathrm{Spec}(B)$.
3. A together with its comultiplication $\Delta\colon A \to A \otimes_R A$ is a (left and right) A-comodule algebra.

Definition 1.1.21 (Morphism of comodule algebras)**.** Let A and A' be R-bialgebras, $\varphi\colon A \to A'$ be a morphism of algebras and C and C' be respectively an A-comodule algebra and an A'-comodule algebra via $\rho\colon C \to C \otimes_R A$ and $\rho\colon C' \to C' \otimes_R A$. We call *morphism of comodule algebras (with respect to φ)* a morphism of algebras $g\colon C \to C'$ that respects the comodule algebra structures, that is the following diagram commutes

$$\begin{array}{ccc} C & \xrightarrow{\quad g \quad} & C' \\ \downarrow{\scriptstyle \rho_C} & & \downarrow{\scriptstyle \rho_{C'}} \\ C \otimes_R A & \xrightarrow{g \otimes \varphi} & C' \otimes_R A'. \end{array}$$

Remark 1.1.22. In the above definition, when C and C' are both A-comodule algebras, one can take φ to be the identity on A. We then have that a *morphism of A-comodule algebras* $g\colon C \to C'$ is an A-linear morphism of algebras, where now A-linearity means that the diagram $\begin{array}{ccc} C & \xrightarrow{\quad g \quad} & C' \\ \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \rho'} \\ C \otimes_R A & \xrightarrow{g \otimes id} & C' \otimes_R A \end{array}$ commutes.

Starting from a left A-module algebra B and a left A-comodule algebra C, one can always construct an algebra $B\#C$ called the *smash product* of B and C, defined as follows.

Definition 1.1.23 (Smash product)**.** Let B be a (left) A-module algebra via

$$\psi\colon A \otimes_R B \to B$$

and C be a (left) A-comodule algebra via

$$\rho\colon C \to A \otimes_R C.$$

We define the R-linear map

$$\begin{aligned}\phi\colon A \otimes_R C \otimes_R B &\to B \otimes_R C \\ a \otimes c \otimes b &\mapsto \psi(a \otimes b) \otimes c = a \cdot b \otimes c.\end{aligned}$$

For $f \in A \otimes_R C$ and $b \in B$ we will denote $f \star b := \phi(f \otimes b)$. The *smash product algebra* $B\#C$ is defined as follows:

1. as an R-module $B\#C = B \otimes_R C$;
2. the multiplication is given by

$$(b \otimes c) \times (\beta \otimes \gamma) = (b \otimes 1)(\rho(c) \star \beta)(1 \otimes \gamma)$$

for any $b, \beta \in B$ and $c, \gamma \in C$.

Example 1.1.24. For B an A-module algebra, one can for example consider the smash product $B\#A$. This will often be the case.

Proposition 1.1.25. *Let A and A' be R-bialgebras, $\varphi\colon A \to A'$ be a morphism of algebras, B and B' be respectively an A-module algebra and an A'-module algebra, C and C' be respectively an A-comodule algebra and an A'-comodule algebra, $f\colon B \to B'$ and $g\colon C \to C'$ be respectively morphisms of (left) module and comodule algebras (with respect to φ). Then $f \otimes g\colon B\#C \to B'\#C'$ is a morphism of algebras.*

Proof. For $c \in C$ let us write $\rho_C(c) = \sum_i a_i \otimes c_i$ where $\rho_C\colon C \to A \otimes_R C$ is the A-comodule structure on C. Recall then that since g is a morphism of module coalgebras it holds $\rho_{C'}(g(c)) = \sum_i \varphi(a_i) \otimes g(c_i)$. Now take $b \otimes c, \beta \otimes \gamma$ in $B\#C$. Then

$$(f \otimes g)((b \otimes c) \times (\beta \otimes \gamma)) = (f \otimes g)\left(\sum_i b(a_i \cdot \beta) \otimes c_i\gamma\right) = \sum_i f(b(a_i \cdot \beta)) \otimes g(c_i\gamma) =$$

$$\sum_i f(b)(\varphi(a_i)) \cdot f(\beta) \otimes g(c_i)g(\gamma) = (f(b) \otimes g(c)) \times (f(\beta) \otimes g(\gamma))$$

as wished. □

Appendix A is devoted to going more in the details of the study of the smash product algebra and of its utility in the context of this work.

Examples around Ore polynomials

This part is devoted to show how the algebra of Ore polynomials (introduced by Ore [Ore33]) can be obtained as a smash product. Let us begin by recalling its definition.

Definition 1.1.26 (θ-derivation)**.** Let R be a commutative ring and $\theta\colon R \to R$ be a morphism of rings. We call *θ-derivation* a linear morphism $\partial\colon R \to R$ such that $\partial(ab) = \theta(a)\partial(b) + \partial(a)b$ for all $a, b \in R$. So if $\theta = \mathrm{id}$, then ∂ is a derivation in the usual sense.

Definition 1.1.27 (Algebra of Ore polynomials)**.** Let R be a commutative ring, $\theta\colon R \to R$ be a morphism of rings and $\partial\colon R \to R$ be a θ-derivation. The *R-algebra of Ore polynomials* $R[X; \theta, \partial]$ has for elements polynomials in X with coefficients in R and multiplication law $a \times X = aX$ and $X \times a = \theta(a)X + \partial(a)$ for every $a \in R$.

Example 1.1.28. Let R be a ring of positive characteristic p and take $\theta = F_R$ the Frobenius morphism on R and $\partial = 0$. Then, there is a ring isomorphism

$$\begin{aligned} R[X; F_R] &\simeq R[T]_{lin} \\ \sum_{i\in\mathbb{N}} a_i X^i &\mapsto \sum_{i\in\mathbb{N}} a_i T^{p^i} \end{aligned}$$

where $R[T]_{lin}$ is the ring of linearised polynomials with coefficients in R, that is polynomials of the form $\sum_{i\in\mathbb{N}} a_i T^{p^i}$ with operations given by the sum and composition of polynomials (these are also known as additive or p-polynomials).

Example 1.1.29.

- **$\mathbb{G}_a$-action.** Consider $A = R[T]$ the Hopf algebra representing the additive group scheme $\mathbb{G}_{a,R}$, that is

$$\Delta(T) = T \otimes 1 + 1 \otimes T, \quad \varepsilon(T) = 0, \quad S(T) = -T.$$

  To give an A-module algebra B is equivalent to defining

$$\begin{aligned} v\colon R[T] &\to \mathrm{End}_R(B) \\ T &\mapsto \partial \end{aligned}$$

  where $\partial(fg) = \partial(f)g + f\partial(g)$, that is it is equivalent to giving an R-linear derivation $\partial\colon B \to B$. The R-algebra structure on the smash product $B\#A$ is given by

$$(1 \otimes T) \times (b \otimes 1) = \Delta(T) \star b = (T \otimes 1 + 1 \otimes T) \star b = \partial(b) \otimes 1 + b \otimes T$$

  for any $b \in B$. Therefore $B\#A \simeq B[T; \partial]$, the algebra of Ore polynomials where multiplication is indeed defined by $Tb = \partial(b) + bT$ for any $b \in B$.

- $\mathbb{G}_m$**-action.** Consider $A = R\left[T, \frac{1}{T}\right]$ the Hopf algebra representing the multiplicative group scheme $\mathbb{G}_{m,R}$, that is

$$\Delta(T) = T \otimes T, \quad \varepsilon(T) = 1, \quad S(T) = \frac{1}{T}.$$

To give an A-module algebra B is equivalent to defining

$$\begin{aligned} v\colon R\left[T, \frac{1}{T}\right] &\to \mathrm{End}_R(B) \\ T &\mapsto \theta \end{aligned}$$

where θ is invertible, that is an automorphism of B. The R-algebra structure on the smash product $B\#A$ is given by

$$(1 \otimes T) \times (b \otimes 1) = \Delta(T) \star b = (T \otimes T) \star b = \theta(b) \otimes T$$

for any $b \in B$. Notice that the algebra of Ore polynomials $B[T; \theta]$, where multiplication is defined by $Tb = \theta(b)T$ for any $b \in B$, is a subalgebra of $B\#A$.

- $\mathbb{G}_{a,R} \rtimes \mathbb{G}_{m,R}$**-action.** Let us consider the semidirect product $\mathbb{G}_{a,R} \rtimes \mathbb{G}_{m,R}$ (where the action of $\mathbb{G}_{m,R}$ on $\mathbb{G}_{a,R}$ is given by multiplication on the left). This group scheme is represented by the Hopf algebra $A = R\left[T, \frac{1}{T}, S\right]$ with comultiplication $\Delta(T) = T \otimes T$ and $\Delta(S) = S \otimes 1 + T \otimes S$. To give an A-module algebra B is equivalent to defining

$$\begin{aligned} v\colon R\left[T, \frac{1}{T}, S\right] &\to \mathrm{Hom}_R(B, B) \\ T &\mapsto \theta, \\ S &\mapsto \partial \end{aligned}$$

where θ is an automorphism of B and $\partial(fg) = \partial(f)g + \theta(f)\partial(g)$ for every $f, g \in B$, that is ∂ is a θ-derivation. The R-algebra structure on the smash product $B\#A$ is given by

$$(1 \otimes T) \times (b \otimes 1) = \Delta(T) \star b = \theta(b) \otimes T$$

and

$$(1 \otimes S) \times (b \otimes 1) = \Delta(S) \star b = (S \otimes 1 + T \otimes S) \star b = \partial(b) \otimes 1 + \theta(b) \otimes S.$$

Notice that the algebra of Ore polynomials $B[S; \partial, \theta]$, where multiplication is defined by

$$Sb = \partial(b) + \theta(b)S$$

for any $b \in B$, is a subalgebra of $B\#A$.

1.2 Nilpotent derivations and p-bases

This part will be devoted to nilpotent derivations, which are often encountered when studying actions of infinitesimal group schemes (see Proposition 3.1.18 and Example 3.1.19). Some of the results appearing here might be known to experts, we have included their proof for lack of a reference. Proposition 1.2.6 and Corollary 1.2.7 will play an important role in the proof of Theorem 3.2.13. A background reference for p-bases is [Bou90, V.§13].

For K a field and D a derivation on K, we denote by K^D the subfield of elements of K annihilated by D, that is

$$K^D := \{x \in K \mid D(x) = 0\}.$$

A derivation D of K is said to be nilpotent of nilpotency index r if $D^r = 0$ and $D^{r-1} \neq 0$, where for any natural n we denote by D^n the composite of D with itself iterated n times. We begin by recalling a fundamental result [Smi68, Theorem 2] showing that nilpotent derivations on fields appear only in characteristic $p > 0$ and that nilpotency indices are always p-powers.

Theorem 1.2.1. *Let D be a non-zero nilpotent derivation of nilpotency index r on a field K. Then K has characteristic $p \neq 0$ and $r = p^t$.*

Proof. By Leibniz formula for every $a, b \in K$ we have

$$0 = D^r(ab) = \sum_{i=0}^{r} \binom{r}{i} D^i(a) D^{r-i}(b).$$

Take $a \in K$ such that $D(a) \neq 0$ and $D^2(a) = 0$: for example one can take $a = D^{r-2}(x)$ where $x \in K$ is such that $D^{r-1}(x) \neq 0$, which exists since $D^{r-1} \neq 0$. Then

$$0 = D^r(ab) = rD(a)D^{r-1}(b)$$

for all $b \in K$ and thus $r = 0$. Therefore K has characteristic $p \neq 0$ and p divides r. Write then $r = qp$. If $q = 1$ we are done. Suppose then that $q > 1$. Then D^p is a non-zero nilpotent derivation on K of index q and repeating the reasoning we deduce that p divides q. Iterating this for a finite number of steps gives the result. □

Definition 1.2.2 (Order of a derivation)**.** Let D be a derivation on a field K. We say that D has *order* r if it is nilpotent of index r.

By Theorem 1.2.1 we have that, if p is a prime number and $t \geq 1$, a derivation D on a field K has order p^t if and only if $D^{p^{t-1}} \neq 0$ and $D^{p^t} = 0$. From now on K will be a field of characteristic $p > 0$ such that the field extension K/K^p is finite (this is the case for example if we take K to be the function field of a variety over a perfect field).

Lemma 1.2.3. *Let D be a derivation on K of order p^n. Then the field extension K/K^D has order p^n, there exists $t \in K$ such that $D(t) = 1$ and $\mathrm{Im}(D^i) = \ker(D^{p^n - i})$ for any $i = 1, \ldots, p^n$.*

Proof. We have that D is a nilpotent K^D-linear map with one-dimensional kernel generated by 1. Therefore there is a unique block in the normal Jordan form of D and it has size p^n, computed with respect to a basis, which we can suppose that contains 1. This implies that $\dim_{K^D} K = p^n$ and there exists t such that $D(t) = 1$. Moreover, since there is only one nilpotent Jordan block, it is clear that $\mathrm{Im}(D^i) = \ker(D^{p^n-i})$ for any $i = 1, \dots, p^n$. □

Definition 1.2.4 (p-basis)**.** Let K/L be a finite field extension such that $K^p \subseteq L$. A *p-basis* of K/L is a sequence $(t_1, \dots, t_n) \in K^n$ such that the monomials $t_1^{m_1} \dots t_n^{m_n}$ with $0 \leq m_1, \dots, m_n \leq p-1$ form an L-basis of K.

Remark 1.2.5.

1. Notice that for any p-basis $(t_1, \dots, t_n)$ of K/L, a derivation D in $\mathrm{Der}_L(K)$ is zero if and only if $D(t_i) = 0$ for all $i = 1, \dots, n$.

2. A sequence $(t_1, \dots, t_n)$ is a p-basis of K/L if and only if $\{dt_1, \dots, dt_n\}$ is a basis of the K-vector space of Kähler differentials $\Omega^1_{K/L}$ [Bou90, V.§13, Theorem 1]. Consider the dual basis $\{\partial_1, \dots, \partial_n\}$, which gives a basis of the K-vector space of derivations $\mathrm{Der}_L(K) = \mathrm{Hom}_K(\Omega^1_{K/L}, K)$. The ∂_i's commute pairwise and satisfy $\partial_i^p = 0$ for all $i = 1, \dots, n$. Moreover $\partial_i(t_j) = \delta_{ij}$.

In the following, we construct special p-bases that can be obtained any time we have a generically free rational action of an infinitesimal commutative unipotent group scheme of height one on a variety (these objects will be defined and the link will be made clear in the following chapters).

Proposition 1.2.6. *Let $D_1, \dots, D_n$ be derivations on K commuting pairwise. Set $K_0 = K$ and $K_j = K^{D_1,\dots,D_j}$ for all $j = 1, \dots, n$. If D_i has order p on K_{i-1} for all $i = 1, \dots, n$ then*

1. *there exists a p-basis $(t_1, \dots, t_n)$ of K/K_n such that $D_i(t_i) = 1$ and $D_i(t_j) = 0$ for all $j > i$. Moreover, $D_i(t_j)$ belongs to K_j for all i and j, and*

2. *$\{D_1, \dots, D_n\}$ is a basis of* $\mathrm{Der}_{K_n}(K)$.

Proof.

1. Consider the tower of extensions

$$K_n \subseteq K_{n-1} \subseteq K_{n-2} \subseteq \cdots \subseteq K_1 \subseteq K.$$

By Lemma 1.2.3, for every $i = 1, \dots, n$ the extension $K_i \subseteq K_{i-1}$ has degree p and there exists $t_i \in K_{i-1}$ such that $D_i(t_i) = 1$, so by degree reasons $K_{i-1} = K_i(t_i)$. Therefore the first statement follows. The second statement is a direct consequence of the first one together with the commutativity hypothesis. Indeed, for every i, j and $h \leq j$ we have

$$D_h(D_i(t_j)) = D_i(D_h(t_j)) = D_i(\delta_{hj}) = 0$$

where δ_{hj} is the Kronecker delta. Hence $D_i(t_j)$ belongs to K_j as claimed.

2. In particular, we see that $[K : K_n] = p^n$. As remarked above, $\mathrm{Der}_{K_n}(K)$ has then dimension n over K, hence it is enough to show that $D_1, \ldots, D_n$ are K-linearly independent. Suppose that they are not and take $a_1, \ldots, a_n$ in K such that

$$a_1 D_1 + \cdots + a_n D_n = 0.$$

Let $i_0 = \max\{i = 1, \ldots, n \mid a_i \neq 0\}$. Then

$$0 = (a_1 D_1 + \cdots + a_n D_n)_{|K_{i_0-1}} = a_{i_0} D_{i_0|K_{i_0-1}}.$$

By assumption D_{i_0} has order p on K_{i_0-1}, so in particular it is different from zero. Thus $a_{i_0} = 0$, which gives a contradiction.

□

We introduce some notation in order to prove the following Corollary that gives necessary and sufficient conditions for some systems of differential equations to have solution. It will play a crucial role for the existence of the generically free actions of Theorem 3.2.13. Let $D_1, \ldots, D_m$ be differential operators on K (see Definition 3.1.16, here the formal definition is not needed, in the following result we will just use the fact that restricted to a certain subfield of K they are derivations) commuting pairwise and $a_1, \ldots, a_m$ be elements of K such that

$$D_i(a_j) = D_j(a_i)$$

for all $i, j = 1 \ldots, m$. Consider moreover a polynomial $F \in (X_1, \ldots, X_m)\, k[X_1, \ldots, X_m]$ and write

$$F = X_1 Q_1 + \cdots + X_m Q_m.$$

We define the differential operator on K

$$\widetilde{F}(a_1, \ldots, a_m) := \sum_{i=1}^{m} a_i Q_i(D_1, \ldots, D_m).$$

Notice that it does not depend on the choice of the Q_i's since $D_i(a_j) = D_j(a_i)$ for every i, j.

Corollary 1.2.7. *Let $D_1, \ldots, D_m$ be differential operators on K as above and set $K_0 = K$ and $K_j = K^{D_1,\ldots,D_j}$ for any $j = 1, \ldots, m$. Suppose moreover that D_i is a derivation of order p^{l_i} on K_{i-1} for any $i = 1, \ldots, m$ and that*

$$D_i^{p^{l_i}} = F_i(D_1, \ldots, D_{i-1})$$

for some polynomial $F_i \in (X_1, \ldots, X_{i-1})k[X_1, \ldots, X_m]$. Then the system

$$\begin{cases} D_1(x) = a_1 \\ \quad \vdots \\ D_m(x) = a_m \end{cases}$$

admits a solution in K, which is unique modulo K_m, if and only if

$$D_i^{p^{l_i}-1}(a_i) = \widetilde{F}_i(a_1, \dots, a_{i-1})$$

for every $i = 1, \dots, m$.

Proof. Suppose that there exists $z \in K$ solution of the above system: then

$$D_i^{p^{l_i}-1}(a_i) = D_i^{p^{l_i}}(z) = F_i(D_1, \dots, D_{i-1})(z) = \widetilde{F}_i(a_1, \dots, a_{i-1})$$

for every $i = 1, \dots, m$. For the other way around, notice that the uniqueness modulo K_m of the solution is clear by the additivity of differential operators: if x and y are both solutions of the system, then $0 = D_i(x) - D_i(y) = D_i(x - y)$ for all $i = 1, \dots, m$, meaning that the two solutions differ by an element of K_m. Let us prove its existence by recursion. Let S_i be the system given by just the first i lines for any $i = 1, \dots, m$. Let us show that if S_i has a solution x_i, then S_{i+1} has a solution. Any solution of S_i is of the form $x_i + y_i$ with $y_i \in K_i$, therefore we wish to find such an element satisfying

$$D_{i+1}(x_i + y_i) = a_{i+1}.$$

This equation is satisfied if and only if

$$D_{i+1}(y_i) = a_{i+1} - D_{i+1}(x_i).$$

For every $j = 1, \dots, i$ we have

$$D_j(D_{i+1}(x_i)) = D_{i+1}(D_j(x_i)) = D_{i+1}(a_j) = D_j(a_{i+1}),$$

that is $a_{i+1} - D_{i+1}(x_i)$ lies in K_i. Moreover,

$$D_{i+1}^{p^{l_{i+1}}-1}(a_{i+1} - D_{i+1}(x_i)) = D_{i+1}^{p^{l_{i+1}}-1}(a_{i+1}) - D_{i+1}^{p^{l_{i+1}}}(x_i) =$$

$$\widetilde{F}_{i+1}(a_1, \dots, a_i) - D_{i+1}^{p^{l_{i+1}}}(x_i) = 0$$

and thus by Lemma 1.2.3 there exists the solution y_i in K_i we were looking for. □

Chapter 2

Finite group schemes

In this chapter we recall some notions and results around finite (commutative) group schemes, with a strong emphasis on infinitesimal commutative unipotent group schemes which have a central role in this thesis (the main background references are [DG70] and [Mil17]). We also introduce the *socle* of a finite group scheme, an object which proves itself helpful when studying generically free or faithful actions of a finite group scheme (see for example Proposition 3.2.1 and Proposition 3.3.1). Moreover, we prove Proposition 2.2.30 giving a description of the Hopf algebra of an infinitesimal commutative unipotent group scheme over a perfect field; this somehow explicit description will further on play a central role for the proof of Theorem 3.2.13 and is very useful in general for constructing actions of this class of group schemes. This first part appears in [Gou23]. The last section is devoted to proving Theorem 2.3.1, which describes explicitly all infinitesimal commutative unipotent group schemes with one-dimensional Lie algebra over an algebraically closed field k.

2.1 Generalities on group schemes

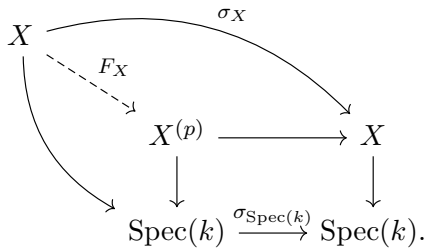
From now on k will denote a ground field of characteristic $p > 0$ and $\overline{k}$ an algebraic closure of k. Moreover, for every k-algebra R and k-scheme X, we denote by X_R the R-scheme $X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(R)$. By *$k$-algebraic* scheme we mean a k-scheme of finite type and we call *k-algebraic group* a k-algebraic group scheme. All the group schemes considered will be algebraic groups. By *k-variety* we mean a separated, geometrically integral k-scheme of finite type and we call *curve* (resp. *surface*) any k-variety of dimension 1 (resp. 2). If X is a k-variety of dimension n, then its function field $K = k(X)$ is a separable, finitely generated extension of k of transcendence degree n. For $G = \mathrm{Spec}(A)$ an affine k-group scheme represented by the Hopf algebra A, we denote by $\Delta\colon A \to A \otimes_k A$ its comultiplication and by $\varepsilon\colon A \to k$ its counit. For G an affine k-group scheme, we also denote by $k[G]$ the Hopf algebra representing it.

Definition 2.1.1 (Absolute Frobenius)**.** Let X be a k-scheme. The *absolute Frobenius morphism* $\sigma_X\colon X \to X$ acts as the identity map on the underlying topological space $|X|$

while on the sections of $\mathcal{O}_X$ over an open subset $U \subseteq X$ it acts as the map

$$\begin{aligned} \mathcal{O}_X(U) &\to \mathcal{O}_X(U), \\ a &\mapsto a^p. \end{aligned}$$

Definition 2.1.2 (Relative Frobenius)**.** Let X be a k-scheme and $X^{(p)} = X \times_{k,f} \operatorname{Spec}(k)$ be the base change with respect to the Frobenius morphism $f\colon k \to k, c \mapsto c^p$ of k. The *relative Frobenius morphism* $F_X\colon X \to X^{(p)}$ is defined by the diagram



We will refer to the relative Frobenius morphism just as the *Frobenius morphism*.

Remark 2.1.3.

1. The assignment $X \mapsto F_X$ is functorial, compatible with fiber products and commutes with extensions of the base field.

2. If X is a scheme over $\mathbb{F}_p$, then $X^{(p)} \simeq X$ and the relative Frobenius F_X coincides with the absolute Frobenius σ_X. Moreover, for any extension $k \supseteq \mathbb{F}_p$ we have $X_k^{(p)} \simeq X_k$ and $F_{X_k} = \sigma_X \times \mathrm{id}_k$.

3. When G is a k-group scheme, then $G^{(p)}$ is also a k-group scheme and the Frobenius morphism $F_G\colon G \to G^{(p)}$ is a homomorphism of group schemes [DG70, II.§7, 1]. If $F_G^n = 0$ for some $n \geq 1$, then G is said to have *height* $\leq n$ and its height is the nilpotency index $\mathrm{ht}(G)$ of F_G.

Proposition 2.1.4. *For any k-variety X, the Frobenius twist $X^{(p)}$ is geometrically integral. Moreover the relative Frobenius $F_X\colon X \to X^{(p)}$ induces a finite extension of function fields $k\left(X^{(p)}\right) \subseteq k(X)$ of degree $p^{\dim(X)}$ and an isomorphism of $k\left(X^{(p)}\right)$ with the composite of the fields k and $(k(X))^p$.*

Proof. See [Liu02, Chapter 3, Corollary 2.27]. □

Definition 2.1.5 (Lie algebra)**.** Let G be an affine k-group scheme and denote by $I_G = \ker(\varepsilon)$ its augmentation ideal (where ε is the counit map $\varepsilon\colon k[G] \to k$). We define the *Lie algebra* of G to be $\mathrm{Lie}(G) = \mathrm{Hom}_k(I_G/I_G^2, k)$. As a k-vector space $\mathrm{Lie}(G)$ is the tangent space of G at the identity element e_G and it has an additional structure of Lie algebra (see for example [DG70, II.§4, 4]).

Remark 2.1.6. Let G be a k-group scheme and $F_G\colon G \to G^{(p)}$ its Frobenius morphism. Then $\mathrm{Lie}(G) = \mathrm{Lie}(\ker(F_G))$ (see [DG70, II.§7, 1.4]).

Definition 2.1.7 (Infinitesimal group scheme)**.** A k-group scheme $G = \mathrm{Spec}(A)$ is said to be *infinitesimal* if its augmentation ideal $I_G = \ker(\varepsilon\colon A \to k)$ is nilpotent.

Example 2.1.8. Two important examples of infinitesimal k-group schemes are given by the kernel of (a power of) the Frobenius morphism of the multiplicative k-group scheme $\mathbb{G}_m$ and of the additive k-group scheme $\mathbb{G}_a$. We obtain respectively

$$\mu_{p^n} := \ker(F^n\colon \mathbb{G}_m \to \mathbb{G}_m) = \mathrm{Spec}\left(k[T]/(T^{p^n}-1)\right)$$

and

$$\alpha_{p^n} := \ker(F^n\colon \mathbb{G}_a \to \mathbb{G}_a) = \mathrm{Spec}\left(k[T]/(T^{p^n})\right)$$

for any $n \geq 1$. Notice that μ_{p^n} and α_{p^n} are isomorphic as k-schemes but not as k-group schemes. Moreover, α_{p^n} is defined only over fields of positive characteristic p, while the subgroup scheme $\mu_n = \mathrm{Spec}\,(k[T]/(T^n-1))$ of $\mathbb{G}_m$ is always well-defined and is étale if $char(k) = 0$ or $(n, char(k)) = 1$.

Notice that non-trivial infinitesimal group schemes exist only over fields of positive characteristic: indeed, by Cartier's Theorem, in characteristic zero all algebraic groups are smooth. Moreover, infinitesimal k-group schemes are group schemes that topologically are just a point: indeed I_G is nilpotent if and only if the topological spaces $|\mathrm{Spec}\, A|$ and $e_G = |\mathrm{Spec}\, A/I_G|$ are isomorphic (and we always have $A/I_G \simeq k$). The structure of the underlying scheme of an infinitesimal group scheme over a perfect field is well-known: we recall it in the following Theorem.

Theorem 2.1.9. *Let k be a perfect field of characteristic $p > 0$ and G be an infinitesimal k-group scheme. Then*

$$k[G] \simeq k[T_1, \ldots, T_r]/(T_1^{p^{e_1}}, \ldots, T_r^{p^{e_r}})$$

for some integers $e_1, \ldots, e_r \geq 1$. In particular $r = \dim_k(\mathrm{Lie}(G))$.

Proof. See [Mil17, Theorem 11.29]. □

Definition 2.1.10 (Unipotent group scheme)**.** A k-algebraic group G is said to be *unipotent* if it is isomorphic to an algebraic subgroup of the k-algebraic group of upper triangular unipotent matrices U_n for some $n \geq 1$.

Definition 2.1.11 (Diagonalizable group scheme/of multiplicative type)**.** An affine k-group scheme G is said to be *diagonalizable* if it is represented by the group-algebra $k[M]$ for some abstract abelian group M, where the k-Hopf algebra structure is given by $\Delta\colon m \mapsto m \otimes m$ and $\varepsilon\colon m \mapsto 1$ for every $m \in M$ (see also Example 1.1.15). It is said to be of *multiplicative type*, if $G_{k^{sep}}$ is diagonalizable for some separable closure k^{sep} of k.

Definition 2.1.12 (Trigonalizable group scheme)**.** A k-group scheme G is said to be *trigonalizable* if it is affine and it has a closed normal unipotent subgroup scheme G^u such that G/G^u is diagonalizable (see for example [DG70, IV.§2, Definition 3.1]).

Let us recall the Theorem of decomposition of commutative affine k-group schemes.

Theorem 2.1.13. *Let G be a commutative affine k-group scheme. Then:*

(i) G has a maximal k-subgroup scheme G^m of multiplicative type and G/G^m is unipotent;

(ii) if k is perfect, G has a maximal unipotent k-subgroup scheme G^u and $G \simeq G^u \times_k G^m$. In particular, G is trigonalizable if and only if G^m is diagonalizable.

Proof. See [DG70, IV.§3, Theorem 1.1]. □

2.2 Finite commutative group schemes

Let $G = \mathrm{Spec}(A)$ be an affine commutative k-group scheme and

$$F_A \colon A^{(p)} = A \otimes_{k,f} k \to A, \quad a \otimes x \mapsto xa^p$$

be the relative Frobenius morphism of A, where f denotes the Frobenius morphism of k. For any k-vector space V, consider the k-vector space of symmetric tensors of order p, $(V^{\otimes p})^{S_p} \subseteq V^{\otimes p}$. Notice that, since G is commutative, A is cocommutative and thus we the map given by the comultiplication $A \to A^{\otimes p}$ factors via $(A^{\otimes p})^{S_p}$:

$$\begin{array}{ccc} A & \longrightarrow & A^{\otimes p} \\ \downarrow & \nearrow & \\ (A^{\otimes p})^{S_p}. & & \end{array}$$

Let $s \colon A^{\otimes p} \to (A^{\otimes p})^{S_p}, a_1 \otimes \cdots \otimes a_p \mapsto \sum_{\sigma \in S_p} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(p)}$ be the symetrization map. By [DG70, IV.§3, 4.1], $(A^{\otimes p})^{S_p}$ is the direct sum of $s(A^{\otimes p})$ and of the submodule generated by $\{a \otimes \cdots \otimes a\}_{a \in A}$. Moreover the canonical map

$$\begin{gathered} \left(A^{\otimes p}\right)^{S_p} / s(A^{\otimes p}) \to A \otimes_{k,f} k \\ a \otimes \cdots \otimes a \mapsto a \otimes 1 \end{gathered}$$

is a bijection.

Definition 2.2.1 (Verschiebung)**.** The *Verschiebung morphism* V_A of A is by definition the composite

$$A \longrightarrow \left(A^{\otimes p}\right)^{S_p} \xrightarrow{\lambda_A} A \otimes_{k,f} k = A^{(p)}$$

where λ_A is the unique k-linear map sending $a \otimes \cdots \otimes a \mapsto a \otimes 1$ for any $a \in A$. The *Verschiebung morphism* $V_G \colon G^{(p)} \to G$ is the homomorphism of group schemes induced by V_A.

Notice that λ_A is well-defined for what was said previously. The assignment $G \mapsto V_G$ is functorial, compatible with fiber products and commutes with extensions of the base field. The Frobenius and the Verschiebung morphisms have both key roles in the theory of finite commutative group schemes.

Remark 2.2.2. For any k-algebra B the multiplication morphism $(B^{\otimes p})^{S_p} \to B$ is given by the composite

$$\left(B^{\otimes p}\right)^{S_p} \xrightarrow{\lambda_B} B^{(p)} \xrightarrow{F_B} B.$$

Moreover, for any k-linear morphism $\varphi\colon B \to C$ we have the commutative diagram

$$\begin{array}{ccc} (B^{\otimes p})^{S_p} & \xrightarrow{\lambda_B} & B^{(p)} \\ \downarrow{\scriptstyle \varphi^{\otimes p}} & & \downarrow{\scriptstyle \varphi^{(p)}} \\ (C^{\otimes p})^{S_p} & \xrightarrow{\lambda_C} & C^{(p)}. \end{array}$$

For more details see [DG70, IV.§3, 4.2]: in loc. cit. the second fact is stated for morphisms of k-algebras but can actually be generalized for any k-linear morphism.

Recall that if (A, Δ, ε) and (B, m, u) are respectively a coalgebra and an algebra over k, then $\mathrm{Hom}_k(A, B)$ has a k-algebra structure with multiplication given by the convolution product

$$\phi \otimes \chi \mapsto m \circ \phi \otimes \chi \circ \Delta$$

and unit

$$k \to \mathrm{Hom}_k(A, B), 1 \mapsto u \circ \varepsilon.$$

Lemma 2.2.3. *Let $G = \mathrm{Spec}(A)$ be an affine commutative k-group scheme, B be a k-algebra and let C denote the k-algebra of k-linear morphisms $\mathrm{Hom}_k(A, B)$. For every element $g \in C^{(p)}$, it holds*

$$F_C(g) = F_B \circ g \circ V_A.$$

Proof. Since F_C is a morphism of k-algebras, it is enough to show the result for g of the form $f \otimes 1 = f^{(p)}$ with $f \in C = \mathrm{Hom}_k(A, B)$. We then have $F_C(f \otimes 1) = f^p$ and we thus wish to show that

$$f^p = F_B \circ f^{(p)} \circ V_A.$$

Using the definition of the convolution product (which is the multiplication law of the algebra C) one sees that the power f^p is equal to the composite

$$A \xrightarrow{comult} \left(A^{\otimes p}\right)^{S_p} \xrightarrow{f^{\otimes p}} \left(B^{\otimes p}\right)^{S_p} \xrightarrow{mult} B.$$

By Remark 2.2.2 we obtain the commutative diagram

$$\begin{array}{ccccccc} A & \xrightarrow{comult} & (A^{\otimes p})^{S_p} & \xrightarrow{f^{\otimes p}} & (B^{\otimes p})^{S_p} & \xrightarrow{mult} & B \\ & \searrow^{V_A} & \downarrow{\scriptstyle \lambda_A} & & \downarrow{\scriptstyle \lambda_B} & \nearrow_{F_B} & \\ & & A^{(p)} & \xrightarrow{f^{(p)}} & B^{(p)} & & \end{array}$$

and thus the statement. □

Recall that a *finite k-group scheme* is a k-group scheme that is finite as a k-scheme and that the category of finite commutative group schemes over a field k is abelian. We call *order* $o(G)$ of a finite k-group scheme $G = \mathrm{Spec}(A)$ the dimension of A as a k-vector space.

Lemma 2.2.4. *Let $G = \mathrm{Spec}(A)$ be a finite (commutative) k-group scheme. Then the dual of A as a k-vector space*

$$A^\vee = \mathrm{Hom}_k(A, k)$$

is a finite dimensional (commutative) k-Hopf algebra.

Proof. [DG70, V.§1.2.10] □

Definition 2.2.5 (Cartier dual)**.** Let G be a finite commutative k-group scheme. We call *Cartier dual* of G the finite commutative k-group scheme

$$G^\vee = \mathrm{Spec}(A^\vee).$$

Remark 2.2.6. The Cartier dual gives an exact contravariant functor from the category of finite commutative k-group schemes to itself. When G is a finite commutative k-group scheme one can verify that the Verschiebung morphism $V_G \colon G^{(p)} \to G$ coincides with the dual of the Frobenius morphism $F_{G^\vee} \colon G^\vee \to (G^\vee)^{(p)} \simeq (G^{(p)})^\vee$ of the Cartier dual $G^\vee$. Moreover it holds $V_G \circ F_G = p_G$ and $F_G \circ V_G = p_{G^{(p)}}$ (see [DG70, IV.§3, 4.9–10] for these two facts).

As we will see in the next chapter, to be able to compute the Cartier dual of a finite group scheme is quite important if we want to explicitly write an action on a variety (see Proposition 3.1.17 and the proof of Theorem 3.2.13). We illustrate a couple of examples to get our hands on how Cartier duals are computed. We start by recalling that if A is a finite dimensional k-Hopf algebra with multiplication m and comultiplication Δ, then the multiplication and comultiplication of $A^\vee$ are respectively given by the convolution product

$$\begin{aligned} m^\vee \colon A^\vee \otimes_k A^\vee &\to A^\vee \\ f \otimes g &\mapsto (A \xrightarrow{\Delta} A \otimes_k A \xrightarrow{f \otimes g} k \otimes_k k \simeq k) \end{aligned}$$

and

$$\begin{aligned} \Delta^\vee \colon A^\vee &\to A^\vee \otimes_k A^\vee \\ \varphi &\mapsto (A \otimes_k A \xrightarrow{m} A \xrightarrow{\varphi} k). \end{aligned}$$

Example 2.2.7.

i) Let us start by computing the dual of $\alpha_p = \mathrm{Spec}\,(k[T]/(T^p))$ where $\Delta(T) = T \otimes 1 + 1 \otimes T$. A basis of $k[\alpha_p]$ as a k-vector space is given by $\{1, T, \dots, T^{p-1}\}$. We then have a dual basis $\{1, T^*, \dots, (T^{p-1})^*\}$ of $k[\alpha_p^\vee]$ over k. Let us compute the comultiplication of $U := T^*$. Using the definition of $\Delta^\vee$ we see that

$$\Delta^\vee(U)(T^i \otimes T^j) = \begin{cases} 1 & \text{if } i+j=1 \\ 0 & \text{otherwise} \end{cases}$$

where $i, j = 0, \dots, p-1$. Therefore, we have $\Delta^\vee(U) = U \otimes 1 + 1 \otimes U$. Using the definition of $m^\vee$ we moreover see that $U^j(T^i) = j!\delta_{ij}$ (where δ_{ij} is the Kronecker delta), that is $U^j = j!(T^j)^*$. As a consequence, it holds $U^p = 0$ and moreover U generates $k[\alpha_p^\vee]$ as a k-algebra. We thus obtain $k[\alpha_p^\vee] = k[U]/(U^p)$ with $\Delta^\vee(U) = U \otimes 1 + 1 \otimes U$, that is α_p is self-dual.

ii) Consider now $G = \mathrm{Spec}\,(k[X,Y]/(X^p, Y^p - X))$ with

$$\begin{aligned} \Delta\colon X &\mapsto X \otimes 1 + 1 \otimes X, \\ Y &\mapsto Y \otimes 1 + 1 \otimes Y - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} X^k \otimes X^{p-k}. \end{aligned}$$

This is the p-torsion of a supersingular elliptic curve when k is algebraically closed (this seems to be a known fact, but we also provide a proof, see Corollary 2.3.10). We see that $\alpha_p = \mathrm{Spec}\,(k[Y]/(Y^p))$ is a k-subgroup scheme of G and thus $k[U]/(U^p)$ is a k-Hopf subalgebra of $k[G^\vee]$ for $U = Y^*$. Consider then $V := X^*$. Using the definition of $\Delta^\vee$ we see that

$$\Delta^\vee(V)(Y^i \otimes Y^j) = \begin{cases} 1 & \text{if } i+j=p \\ 0 & \text{otherwise} \end{cases}$$

where $i, j = 0, \dots, p^2 - 1$. Therefore, we have

$$\begin{aligned} \Delta^\vee(V) &= V \otimes 1 + 1 \otimes V + \sum_{k=1}^{p-1} (Y^k)^* \otimes (Y^{p-k})^* \\ &= V \otimes 1 + 1 \otimes V + \sum_{k=1}^{p-1} \frac{1}{k!(p-k)!} (Y^*)^k \otimes (Y^*)^{p-k} \\ &= V \otimes 1 + 1 \otimes V - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} (Y^*)^k \otimes (Y^*)^{p-k}. \end{aligned}$$

Moreover one sees that $V^j = j!(X^*)^j$ for $j = 1, \dots, p-1$ and that $V^p = Y^*$: indeed

$$V^p(Y) = m(V \otimes V^{p-1}(\Delta(Y))) = m(V \otimes V^{p-1}(-X \otimes X^{p-1})) = 1$$

and $V^p(Y^j) = 0$ for $j \neq 1$. We have thus shown that $k[G^\vee] = k[U,V]/(U^p, V^p - U)$, that is G is also self-dual.

iii) Let M be a finite abstract abelian group and $k[M]$ be the group-algebra with its Hopf algebra structure $\Delta\colon m \mapsto m \otimes m$ for every $m \in M$. A basis of $k[M]$ as a k-vector space is given by $\{m \mid m \in M\}$ and thus, if we consider its dual $k[M]^\vee$, a basis is given by $\{e_m\colon k[M] \to k, n \mapsto \delta_{mn}\}$, where δ_{mn} is the Kronecker delta. Using the definition of $\Delta^\vee$ we see that $\Delta^\vee(e_m) = \sum_{n\in M} e_n \otimes e_{m-n}$. So we showed that the dual of any finite diagonalizable k-group scheme $\operatorname{Spec}(k[M])$ is the constant k-group scheme $\underline{M}_k = \operatorname{Spec}\left(k^M\right)$. For example, for any $n \geq 2$, we have $\mu_{n,k}^\vee = (\operatorname{Spec} k[\mathbb{Z}/n\mathbb{Z}])^\vee \simeq \underline{\mathbb{Z}/n\mathbb{Z}}_k$.

For G a finite commutative k-group scheme, we denote by G^0 the k-subgroup scheme of G given by the connected component of the identity element and by G^{red} the reduced closed subscheme of G with the same support. If k is perfect, then G^{red} is a k-subgroup scheme of G and $G \simeq G^0 \times_k G^{red}$. We say that G is *local* (equivalently *infinitesimal* or *connected*) if $G = G^0$ and that it is *reduced* (equivalently *étale*) if $G = G^{red}$. Moreover, we say that G is of *x-y type* if G has the property of being x and its dual has the property of being y. For finite commutative group schemes over a perfect field we have the following decomposition result.

Theorem 2.2.8. *Let k be a perfect field of positive characteristic p. For G a finite commutative k-group scheme, there is a unique functorial decomposition*

$$G = G_{rr} \times_k G_{rl} \times_k G_{lr} \times_k G_{ll}$$

where the direct summands are of reduced-reduced, reduced-local, local-reduced, local-local type respectively.

Proof. The decomposition $G \simeq G^0 \times_k G^{red}$ is functorial, therefore $G^\vee \simeq (G^0)^\vee \times_k (G^{red})^\vee$. Decomposing each factor in its connected and reduced components and dualizing back we obtain the claim. □

We also have the following characterizations.

Proposition 2.2.9. *Let G be a finite commutative k-group scheme.*

1. *The following are equivalent:*
   - *(a) G is étale,*
   - *(b) F_G is an isomorphism,*
   - *(c) $V_{G^\vee}$ is an isomorphism,*
   - *(d) $G^\vee$ is of multiplicative type.*
2. *The following are equivalent:*
   - *(a) G is infinitesimal,*
   - *(b) F_G is nilpotent,*
   - *(c) $V_{G^\vee}$ is nilpotent,*
   - *(d) $G^\vee$ is unipotent.*

Proof. See [DG70, IV.§3, 5.3]. □

Therefore, over a perfect field, we have that

G is of type	reduced-reduced if and only if it is étale of multiplicative type reduced-local if and only if it is étale unipotent local-reduced if and only if it is infinitesimal of multiplicative type local-local if and only if it is infinitesimal unipotent.

Infinitesimal commutative unipotent group schemes

We begin with a useful lemma on infinitesimal group schemes.

Lemma 2.2.10. *Let G be an infinitesimal k-group scheme of order p^n for some $n \geq 0$. Then:*

i) $\max\left(\dim_k(\mathrm{Lie}(G)), \mathrm{ht}(G)\right) \leq n$;

ii) $n \leq \dim_k(\mathrm{Lie}(G)) \times \mathrm{ht}(G) \leq n \times \min\left(\dim_k(\mathrm{Lie}(G)), \mathrm{ht}(G)\right)$;

iii) if G is also commutative and unipotent then also $V_G^n = 0$, where V_G is the Verschiebung morphism.

Proof. We can suppose that k is perfect. Then by Theorem 2.1.9 we have

$$k[G] \simeq k[T_1, \ldots, T_s]/(T_1^{p^{e_1}}, \ldots, T_s^{p^{e_s}})$$

as k-algebras where $1 \leq e_1 \leq \cdots \leq e_s$, $e_1 + \cdots + e_s = n$, $e_s = \mathrm{ht}(G)$ and $s = \dim_k(\mathrm{Lie}(G))$. The first two points then follow, indeed

i) $n = e_1 + \cdots + e_s \geq s = \dim_k(\mathrm{Lie}(G))$ and $n = e_1 + \cdots + e_s \geq e_s = \mathrm{ht}(G)$ yielding that $n \geq \max(\dim_k(\mathrm{Lie}(G)), \mathrm{ht}(G))$; and

ii) $n = e_1 + \cdots + e_s \leq s \times e_s = \dim_k(\mathrm{Lie}(G)) \times \mathrm{ht}(G) \leq n \times \min\left(\dim_k(\mathrm{Lie}(G)), \mathrm{ht}(G)\right)$ where the second inequality follows from the first point.

iii) If G is infinitesimal commutative unipotent, then its dual $G^\vee$ is also such and has order p^n. Then, applying the first statement, we have $F_{G^\vee}^n = 0$ and thus $V_G^n = 0$.

□

Remark 2.2.11. Notice that, by the second statement of the above Lemma, we have in particular that $\dim_k(\mathrm{Lie}(G)) = 1$ if and only if $\mathrm{ht}(G) = n$ and that $\mathrm{ht}(G) = 1$ if and only if $\dim_k(\mathrm{Lie}(G)) = n$.

The group scheme of Witt vectors W over a perfect field k of positive characteristic p plays a central role in the study of unipotent commutative k-group schemes. We thus recall here some of its main properties that will be used freely later on. A reference for this is [DG70, V.§1 and §4]. As a k-scheme, W coincides with $\mathbb{A}_k^{\mathbb{N}}$ and it is endowed with a structure of ring scheme coming from Witt polynomials. We will mostly be interested in its structure of group scheme. We denote by W_n the k-subgroup scheme of W of

Witt vectors of length $\leq n$ and by W_n^m the kernel of $F^m\colon W_n \to W_n$ (where F is the Frobenius morphism of W_n). As a k-scheme, W_n coincides with $\mathbb{A}_k^n$ and we denote by $k[T_0, \dots, T_{n-1}]$ its k-Hopf algebra. Notice that if we want to consider r copies of W_n we will use the notation $(W_n)^r$ with the parenthesis. The k-group scheme W_n^m is the Cartier dual of W_m^n for every $n, m \geq 1$. If for example we consider (x_0, x_1) and (y_0, y_1) two Witt vectors of length 2, then their sum is given by

$$(x_0, x_1) + (y_0, y_1) = (x_0 + y_0, x_1 + y_1 + S_1(x_0, y_0))$$

where $S_1(x_0, y_0) = -\sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} x_0^k y_0^{p-k}$. In general the expression for the sum of Witt vectors gets more complicated with the increasing of the length. One important property is that, if we give weight p^j to the jth coordinate for any $j \in \mathbb{N}$, then the polynomial expressing the ith term of the sum is homogeneous of degree p^i; moreover it involves just the coordinates of the vectors up to the index i. Notice that W is defined over $\mathbb{F}_p$ and thus $W^{(p)} \simeq W$. Let V be the Verschiebung morphism of W_n. On points F and V act as follows:

$$F\left((x_0, x_1, \dots, x_{n-1})\right) = (x_0^p, x_1^p, \dots, x_{n-1}^p)$$

and

$$V\left((x_0, x_1, \dots, x_{n-1})\right) = (0, x_0, x_1, \dots, x_{n-2}).$$

Moreover $F \circ V = V \circ F = p \cdot \mathrm{id}$, therefore

$$p \cdot (x_0, x_1, \dots, x_{n-1}) = (0, x_0^p, x_1^p, \dots, x_{n-2}^p).$$

Proposition 2.2.12. *If k is perfect, then every infinitesimal commutative unipotent k-group scheme G can be embedded in $(W_n^m)^r$ for some $n, m, r \geq 1$.*

Proof. See [DG70, V.§1, Proposition 2.5]. □

Remark 2.2.13. Recall that a finite commutative k-group scheme is infinitesimal unipotent if and only if its Frobenius and Verschiebung morphisms are both nilpotent (Proposition 2.2.9). In particular, in Proposition 2.2.12 one can take m and n to be respectively their nilpotency indices (this is a direct consequence of the functoriality of the Frobenius and Verschiebung morphism).

The collection of W_n^m becomes a direct system with index set $\mathbb{N} \times \mathbb{N}$ via the homomorphisms

$$\begin{array}{ccc} W_n^m & \xhookrightarrow{i} & W_n^{m+1} \\ \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle v} \\ W_{n+1}^m & \xhookrightarrow{i} & W_{n+1}^{m+1} \end{array}$$

where v and i are the monomorphisms induced naturally by the Verschiebung and the inclusion respectively. Let $\sigma\colon W(k) \to W(k)$ be the ring endomorphism induced by the Frobenius morphism F.

Definition 2.2.14. We will denote by E the ring of non-commutative polynomials over the ring $W(k)$ in two variables $\mathbb{F}$ and $\mathbb{V}$ subject to the following relations:

- $\mathbb{F} \cdot \xi = \sigma(\xi) \cdot \mathbb{F}$ for all $\xi \in W(k)$;
- $\mathbb{V} \cdot \sigma(\xi) = \xi \cdot \mathbb{V}$ for all $\xi \in W(k)$;
- $\mathbb{F}\mathbb{V} = \mathbb{V}\mathbb{F} = p$.

Notice that E is a free left (or right) $W(k)$-module with basis $\{\dots, \mathbb{V}^2, \mathbb{V}, 1, \mathbb{F}, \mathbb{F}^2, \dots\}$ (see [DG70, V.§1, 3]).

Proposition 2.2.15. *There exists a unique ring homomorphism $E \to \mathrm{End}(W_n^m)$ for all n, m such that $\mathbb{F}$ and $\mathbb{V}$ act as the Frobenius and the Verschiebung morphisms and $\xi \in W(k)$ acts through multiplication by $\sigma^{-n}(\xi)$. These actions of E are compatible with the homomorphisms i and v of the directed system.*

Proof. See [DG70, V.§1, 3.4]. □

Definition 2.2.16 (Dieudonné module)**.** For any infinitesimal commutative unipotent k-group scheme, we define

$$M(G) := \varinjlim_{n,m} \mathrm{Hom}(G, W_n^m)$$

with left E-module structure given by the action of E on W_n^m, called *Dieudonné module of* G. Then M is a left exact additive functor from the category of infinitesimal commutative unipotent k-group schemes to that of left E-modules.

Theorem 2.2.17. *The functor M induces an anti-equivalence of categories between the category of infinitesimal commutative unipotent k-group schemes to that of left E-modules of finite length with F and V nilpotent.*

Proof. See [DG70, V.§1, Theorem 4.3] or [Pin05, Theorem 23.2]. □

The socle of a finite group scheme

In the context of group theory, the *socle* of a finite abstract group G is the subgroup generated by the non-trivial minimal normal subgroups of G. We introduce here a generalization to finite group schemes of this classical definition; for this idea we are thankful to Michel Brion.

Definition 2.2.18 (Socle)**.** For G a finite k-group scheme, we define the *socle* of G, denoted $\mathrm{soc}(G)$, to be the k-subgroup scheme generated by the non-trivial minimal normal k-subgroup schemes of G.

The following Lemma describes some properties of the socle of a finite group scheme.

Lemma 2.2.19. *Let G be a finite k-group scheme.*

1. *G is non-trivial if and only if* $\mathrm{soc}(G)$ *is non-trivial.*
2. $\mathrm{soc}(G)$ *is a normal k-subgroup scheme of G.*
3. $\mathrm{soc}(G) \times_G H$ *is non-trivial for any non-trivial normal k-subgroup scheme H of G.*
4. *If G is commutative, then* $\mathrm{soc}(H) = \mathrm{soc}(G) \times_G H$ *for any k-subgroup scheme $H \subseteq G$, in particular* $\mathrm{soc}(\mathrm{soc}(G)) = \mathrm{soc}(G)$.
5. *If G is infinitesimal, then* $\mathrm{soc}(G) \subseteq \mathrm{soc}(\ker(F_G))$. *If in addition G is commutative, then* $\mathrm{soc}(G) = \mathrm{soc}(\ker(F_G))$.
6. *If G_1 and G_2 are finite commutative k-group schemes, then*
$$\mathrm{soc}(G_1 \times_k G_2) = \mathrm{soc}(G_1) \times_k \mathrm{soc}(G_2).$$
7. *For any morphism of finite commutative k-group schemes $G_1 \to G_2$, the induced morphism* $\mathrm{soc}(G_1) \to G_2$ *factors via* $\mathrm{soc}(G_2)$.

Proof.

1. Since G is normal in itself and it is finite, there exist non-trivial minimal normal subgroup schemes.
2. Clear by definition since the socle is generated by non-trivial normal subgroup schemes.
3. Since G is finite we may suppose that H is minimal, hence $\mathrm{soc}(G) \times_G H = H$.
4. Notice that since G is commutative any of its subgroup schemes is normal. A non-trivial minimal k-subgroup scheme of H is also a minimal k-subgroup scheme of G. Therefore $\mathrm{soc}(H) \subseteq \mathrm{soc}(G) \times_G H$. Let N be a non-trivial minimal k-subgroup scheme of G. By minimality, either N is a k-subgroup scheme of H or $N \times_G H$ is trivial. Suppose the former. Then N is also a minimal k-subgroup scheme of H. Therefore the equality.
5. Let N be a non-trivial minimal normal k-subgroup scheme of G. Since G is infinitesimal, then $N \times_G \ker(F_G) = \ker(F_N)$ is a non-trivial normal k-subgroup scheme of G. Therefore, by minimality, N is a k-subgroup scheme of $\ker(F_G)$. Hence $\mathrm{soc}(G) \subseteq \mathrm{soc}(\ker(F_G))$. If G is commutative, by the previous point also the other inclusion holds.
6. Clearly $\mathrm{soc}(G_1 \times_k G_2)$ is contained in $\mathrm{soc}(G_1) \times_k \mathrm{soc}(G_2)$. Take now $N_1 \times_k N_2$ with N_i non-trivial minimal k-subgroup scheme of G_i. Then N_i is also a minimal k-subgroup scheme of $G_1 \times_k G_2$ (notice that again we are using the assumption that the G_i's are commutative). Therefore, by definition of the socle subgroup scheme, $N_1 \times_k N_2 \subseteq \mathrm{soc}(G_1 \times_k G_2)$ and thus also the inverse inclusion holds true.

7. Let N be a non-trivial minimal k-subgroup scheme of G_1, then N is mapped to a minimal k-subgroup scheme of G_2.

□

Before giving the following definitions, let us recall that $\mathrm{End}(\alpha_p) = k$ and $\mathrm{End}(\mu_p) = \mathbb{F}_p$. As a consequence, we have that $\mathrm{Hom}(\alpha_p, G)$ and $\mathrm{Hom}(\mu_p, G)$ have respectively a natural structure of k-vector space and of $\mathbb{F}_p$-vector space, for any k-group scheme G.

Definition 2.2.20 (a-number)**.** Let k be perfect and G be a commutative trigonalizable k-group scheme. The *a-number* of G is $\dim_k(\mathrm{Hom}(\alpha_p, G))$.

Remark 2.2.21. Notice that the a-number of G coincides also with the maximal natural number r such that G contains a k-subgroup scheme isomorphic to α_p^r. In addition to that, the a-number of G is zero if and only if G is diagonalizable, since any non-trivial unipotent group scheme contains a k-subgroup scheme isomorphic to α_p.

Definition 2.2.22 (p-rank)**.** Let k be perfect and G be a commutative trigonalizable k-group scheme. The *p-rank* of G is $\dim_{\mathbb{F}_p}(\mathrm{Hom}(\mu_p, G))$.

Remark 2.2.23. Notice that the p-rank of G coincides also with the maximal natural number n such that G contains a k-subgroup scheme isomorphic to μ_p^n. In addition to that, the p-rank of G is zero if and only if G is unipotent.

Lemma 2.2.24. *If k is perfect and G is an infinitesimal commutative unipotent k-group scheme, then the following are equivalent:*

(i) r is the a-number of G;

(ii) r is the minimal natural number such that for any closed immersion $G \subseteq (W_n^m)^s$ there exists a projection $(W_n^m)^s \twoheadrightarrow (W_n^m)^r$, which forgets $s - r$ copies of W_n^m, inducing an immersion of G in $(W_n^m)^r$.

Moreover the following facts hold true:

(a) $\mathrm{soc}(G) \simeq \alpha_p^r$ and, in particular, $\mathrm{soc}(G)$ is the maximal k-subgroup scheme of $\ker(F_G)$ with trivial Verschiebung;

(b) $r \leq \min\left(\dim_k(\mathrm{Lie}(G)), \dim_k(\mathrm{Lie}(G^\vee))\right)$ and $\dim_k(\mathrm{Lie}(G)) = r$ if and only if $\ker(F_G)$ is isomorphic to α_p^r.

Proof.

$(i) \Rightarrow (ii)$ Let r be the a-number of G, that is r is the maximal natural number r such that G contains a k-subgroup scheme H isomorphic to α_p^r. By Proposition 2.2.12 there exists an embedding $G \subseteq (W_n^m)^s$ for some $s \geq 1$. Notice that since $H \subseteq G$ is annihilated both by the Frobenius and the Verschiebung, then

$$\alpha_p^r \simeq H \subseteq \left(W_1^1\right)^s = \alpha_p^s$$

and thus $s \geq r$. If $s = r$ we are done. Suppose that $s > r$, then there exists a projection $(W_n^m)^s \twoheadrightarrow (W_n^m)^{s-1}$ forgetting a copy of W_n^m which induces an immersion $G \hookrightarrow (W_n^m)^{s-1}$. Indeed, suppose that all the projections

$$\pi_i \colon G \to (W_n^m)^{s-1}$$

have non-trivial kernel $\ker(\pi_i)$. Then $\ker(\pi_i)$ is a non-trivial k-subgroup scheme of G for every $i = 1, \ldots, s$ and thus it contains a k-subgroup scheme isomorphic α_p. Since each $\ker(\pi_i)$ lies in a different copy of W_n^m, we therefore have s linearly independent homomorphisms $\alpha_p \hookrightarrow G$, contradicting the fact that the a-number of G is $r < s$. Now again, if $s - 1 = r$ we are done, otherwise we repeat the same reasoning until reaching r. Clearly r is minimal for this property since α_p^r is not isomorphic to a k-subgroup scheme of $(W_n^m)^{r-1}$.

$(ii) \Rightarrow (i)$ By minimality of r all the projections

$$\pi_i \colon G \to (W_n^m)^{r-1}$$

have non-trivial kernel $\ker(\pi_i)$. Then $\ker(\pi_i)$ is a non-trivial k-subgroup scheme of G for every $i = 1, \ldots, s$ and thus it contains a k-subgroup scheme isomorphic to α_p. So for every $i = 1, \ldots, r$ we have a different copy of α_p contained in G, since each $\ker(\pi_i)$ lies in a different copy of W_n^m. Therefore G contains a k-subgroup scheme isomorphic to α_p^r and clearly r is maximal for this property since α_p^{r+1} is not isomorphic to a k-subgroup scheme of $(W_n^m)^r$.

(a) Let r be the a-number of G. Then there are r linearly independent homomorphisms $\alpha_p \hookrightarrow G$ and each α_p is a minimal normal k-subgroup scheme of G. Therefore $\mathrm{soc}(G) = \mathrm{soc}(\ker(F_G))$ contains a k-subgroup scheme isomorphic to α_p^r. On the other hand, all the minimal normal subgroups of $\ker(F_G)$ are copies of α_p (see [DG70, VI.§2, Proposition 2.5]), thus $\mathrm{soc}(\ker(F_G)) = \alpha_p^s$ for some $s \geq 1$. Combining the previous inclusion and the maximality of r we obtain the equality. Suppose that H is a k-subgroup scheme of $\ker(F_G)$ with trivial Verschiebung. Then $H \subseteq \mathbb{G}_a^{s'}$ for some $s' \geq 1$ (see [DG70, IV.§3, Theorem 6.6]) and by the first point we can suppose that s' is the maximal natural number such that H contains a k-subgroup scheme isomorphic to $\alpha_p^{s'}$. Since $H \subseteq \ker(F_G)$, then $H = \ker(F_H)$. Moreover $\dim_k(\mathrm{Lie}(H)) = s'$ and thus by order reasons we have $H = \ker(F_H) \simeq \alpha_p^{s'}$. By maximality of r, $H \subseteq \mathrm{soc}(G) \simeq \alpha_p^r$.

(b) Let r be the a-number of G, then $\dim_k(\mathrm{Lie}(G)) \geq r$. By assumption G contains a k-subgroup scheme H isomorphic to α_p^r. Dualizing, we obtain the faithfully flat homomorphism

$$G^\vee \twoheadrightarrow H \simeq \alpha_p^r$$

and thus $r \leq \dim_k(\mathrm{Lie}(G^\vee))$. The inequality is given by [BM11, Proposition 2.5] which states that if we have a flat local morphism $A \to B$ of Noetherian local rings with maximal ideal and residue field respectively m_A, m_B and $\kappa(A), \kappa(B)$,

then $\dim_{\kappa(A)}\left(m_A/m_A^2\right) \leq \dim_{\kappa(B)}\left(m_B/m_B^2\right)$. For the last statement, clearly if $\ker(F_G) \simeq \alpha_p^r$ then $\dim_k(\mathrm{Lie}(G)) = r$. Now, by assumption we have $\alpha_p^r \simeq H \subseteq G$, so in particular $\alpha_p^r \simeq H \subseteq \ker(F_G)$, and if $\dim_k(\mathrm{Lie}(G)) = r$ the equality must hold since in this case H and $\ker(F_G)$ have both order p^r.

□

As a direct consequence, along with Lemma 2.2.10, we have the following.

Corollary 2.2.25. *If k is perfect, G is an infinitesimal commutative unipotent k-group scheme of order p^n, $G^\vee$ its Cartier dual and*

$$\min(\dim_k(\mathrm{Lie}(G)), \dim_k(\mathrm{Lie}(G^\vee))) = 1,$$

then both G and $G^\vee$ embed in just one copy of the k-group scheme of Witt vectors, more precisely in W_n^n.

Lemma 2.2.26. *Let G be an infinitesimal commutative k-group scheme.*

1. *If $\ker(F_G)$ is diagonalizable, then $\mathrm{soc}(G) = \ker(F_G) = \mu_p^n$, where n is the p-rank of G.*

Moreover, if k is perfect and G is trigonalizable:

2. *$\mathrm{soc}(G) \simeq \alpha_p^r \times_k \mu_p^n$, where r is the a-number of G and n is the p-rank of G. In particular,*
$$\mathrm{soc}(G) = (\ker(F_G) \times_G \ker(V_{G^{(1/p)}})) \times_k \ker(F_{G/G^u}).$$
3. *$\mathrm{soc}(G) \times_k K = \mathrm{soc}(G_K)$ for any field extension K/k.*

Proof.

1. By assumption $\ker(F_G) = \mu_p^n$ where n is the maximal natural number such that $\mu_p^n \subseteq G$. Then, by Lemma 2.2.19, $\mathrm{soc}(G) = \mathrm{soc}(\ker(F_G)) = \mu_p^n$.

2. Since k is perfect, then $G \simeq G^u \times_k G/G^u$ and by Lemma 2.2.19
$$\mathrm{soc}(G) \simeq \mathrm{soc}(G^u) \times_k \mathrm{soc}(G/G^u).$$
Therefore the first part of the statement follows by 1. and Lemma 2.2.24. We have already proved that $\mathrm{soc}(G/G^u) = \ker(F_{G/G^u})$. It is then enough to prove that
$$\alpha_p^r \simeq \mathrm{soc}(G^u) = \ker(F_G) \times_G \ker(V_{G^{(1/p)}}).$$
The left to right inclusion is clear. By Lemma 2.2.24, $G^u \subseteq (W_n^m)^r$. Hence,
$$\ker(F_G) \times_G \ker(V_{G^{(1/p)}}) \subseteq (W_n^1)^r \times_{(W_n^m)^r} (W_1^m)^r = (W_1^1)^r = \alpha_p^r.$$
The claimed equality then holds.

3. If K is perfect, the statement is a direct consequence of the compatibility of Frobenius and Verschiebung kernels with respect to base change. For the general case, clearly $\mathrm{soc}(G) \times_k K \subseteq \mathrm{soc}(G_K)$. Let K^{perf} be the perfect closure of K. Then we have
$$\mathrm{soc}(G) \times_k K^{perf} \hookrightarrow \mathrm{soc}(G_K) \times_K K^{perf} \hookrightarrow \mathrm{soc}(G_{K^{perf}})$$
and the first and last term coincide. Therefore $\mathrm{soc}(G) \times_k K^{perf} \simeq \mathrm{soc}(G_K) \times_K K^{perf}$ and so the inclusion $\mathrm{soc}(G) \times_k K \subseteq \mathrm{soc}(G_K)$ is in fact an equality.

□

Remark 2.2.27. Let k be perfect, G be a commutative trigonalizable k-group scheme and G^u be its maximal unipotent k-subgroup scheme. The *a-number* of G coincides with the dimension of $\mathrm{Lie}(\mathrm{soc}(G^u))$.

Example 2.2.28.

1. $\mathrm{soc}\left((W_n^m)^s\right) = \alpha_p^s$ for all $n, m, s \geq 1$ and $\mathrm{soc}(G) = \alpha_p$ for any non-trivial $G \subseteq W_n^m$ and the a-numbers are respectively s and 1.

2. Let k be algebraically closed and A be an abelian variety of dimension g defined over k. The p-torsion $A[p]$ is a finite commutative k-group scheme annihilated by p with rank p^{2g}. The *p-rank* of A is
$$f = \dim_{\mathbb{F}_p}(\mathrm{Hom}(\mu_p, A[p])).$$
The *a-number* of A is
$$a = \dim_k \left(\mathrm{Hom}(\alpha_p, A[p])\right).$$
Let $A[p]^0$ be the identity component of $A[p]$ and $A[p]^{0,u}$ its unipotent part. It is known that
$$A[p] = A[p]^{0,u} \times_k \mu_p^f \times_k (\mathbb{Z}/p\mathbb{Z})^f$$
(see for example [Mum08, p. III.15]). Then $\mathrm{soc}(A[p]) = \alpha_p^a \times_k \mu_p^f \times (\mathbb{Z}/p\mathbb{Z})^f$ and the a-number of A coincides with $\dim_k \left(\mathrm{Lie}\left(\mathrm{soc}\left(A[p]^{0,u}\right)\right)\right)$ or equivalently it is the maximal natural number a such that $A[p]$ contains a k-subgroup scheme isomorphic to α_p^a.

Young diagrams for commutative unipotent group schemes of height one

Let k be perfect and G be a commutative unipotent k-group scheme of height one, then $G \simeq \prod_{i=1}^s W_{n_i}^1$ for some $s, n_i \geq 1$ (see [DG70, IV.§2, 2.14]). Moreover, we may suppose that $n_1 \geq \cdots \geq n_s$. We can then encode any such group scheme by a Young diagram $\tau(G)$, namely the one of shape $(n_1, \ldots, n_s)$. For example

$$\tau(\alpha_p) = \ydiagram{1}, \quad \tau(W_3^1 \times_k \alpha_p) = \ydiagram{3,1}, \quad \tau(W_2^1 \times_k W_2^1) = \ydiagram{2,2}.$$

The following lemma lists some straightforward properties, we thus omit the proof.

Lemma 2.2.29.

- *Two commutative unipotent k-group schemes of height one are isomorphic if and only if their Young diagrams coincide.*
- *The first column of $\tau(G)$ coincides with $\tau(\mathrm{soc}(G))$.*
- *The first n columns represent $\tau(\ker(V_G^n))$ and the length of the nth column corresponds to the maximal r such that G contains a k-subgroup scheme isomorphic to $\left(W_n^1\right)^r$.*
- *The dimension of the Lie algebra of G and $\log_p(o(G))$ both coincide with the number of boxes of $\tau(G)$.*

Given $G_1, \dots, G_l$ commutative unipotent k-group schemes of height one, the smallest commutative unipotent k-group scheme G of height one containing all of them corresponds to the smallest Young diagram containing $\tau(G_i)$ for all i. Explicitly, if $\tau(G_i) = (n_{1i}, \dots, n_{s_i i})$ for some $s_i \geq 1$ and for $i = 1, \dots, l$ then $\tau(G) = (n_1, \dots, n_s)$ where $s = \max\{s_1, \dots, s_l\}$ and $n_j = \max\{n_{j1}, \dots, n_{jl}\}$ for every $j = 1, \dots, s$. For example, if we take $G_1 = W_3^1 \times_k \alpha_p$ and $G_2 = W_2^1 \times_k W_2^1$, then $\tau(G) = \begin{array}{|c|c|c|}\hline \ & \ & \ \\ \hline \ & \ \\ \cline{1-2}\end{array}$ and $G = W_3^1 \times_k W_2^1$.

Algebraic description of infinitesimal commutative unipotent group schemes

In the last part of this section we give a description of the Hopf algebra of an infinitesimal commutative unipotent group scheme over a perfect field. This result will be crucial for the proof of Theorem 3.2.13. Let k be perfect and G be a commutative unipotent k-algebraic group. Then $V_G^n = 0$ for some nilpotency index $n \geq 1$. We then have the cofiltration

$$G = G/\operatorname{Im}(V_G^n) \to G/\operatorname{Im}(V_G^{n-1}) \to \cdots \to G/\operatorname{Im}(V_G) \to 0.$$

We call G_i the k-group scheme $G/\operatorname{Im}(V_G^i)$ and H_i the kernel of the map $G_i \to G_{i-1}$. Notice that then $H_i = \operatorname{Im}(V_G^{i-1})/\operatorname{Im}(V_G^i)$ and thus is killed by the Verschiebung. If G is infinitesimal, then $H_i \simeq \prod_{j=1}^{r_i} \alpha_{p^{l_{ij}}}$ for some $r_i \geq 1$ and $l_{i1}, \dots, l_{ir_i} \geq 1$. Moreover, there are epimorphisms $H_i^{(p)} \to H_{i+1}$ induced by $V_G\colon \left(\operatorname{Im}(V_G^{i-1})\right)^{(p)} \to \operatorname{Im}(V_G^i)$. In particular, the order and the dimension of the Lie algebra of the H_i's are decreasing (the latter is given by [BM11, Proposition 2.5], applied as explained at the end of the proof of Lemma 2.2.24).

Proposition 2.2.30. *Let k be perfect, G be an infinitesimal commutative unipotent k-group scheme and n be the nilpotency index of V_G. For all $i = 1, \dots, n$ let $G_i = G/\operatorname{Im}(V_G^i)$, $H_i = \operatorname{Im}(V_G^{i-1})/\operatorname{Im}(V_G^i)$ and $r_i = \dim_k(\mathrm{Lie}(H_i))$. Then, for all $i = 1, \dots, n$, there exist integers $l_{i1}, \dots, l_{ir_i} \geq 1$, a k-group scheme $\mathcal{G}_i$ and a commutative diagram*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H_i & \longrightarrow & G_i & \longrightarrow & G_{i-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\
0 & \longrightarrow & \mathbb{G}_a^{r_i} & \longrightarrow & \mathcal{G}_i & \longrightarrow & G_{i-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{G}_a^{r_i} & \xrightarrow{\mathrm{id}} & \mathbb{G}_a^{r_i} & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

with exact rows and columns, where $\phi = (F_{\mathbb{G}_a}^{l_{ij}})$. *Moreover, the* k*-Hopf algebra of* $\mathcal{G}_i$ *is*

$$k[\mathcal{G}_i] = k[G_{i-1}][T_{i1}, \ldots, T_{ir_i}]$$

with comultiplication extending that of $k[G_{i-1}]$ *and such that*

$$\Delta(T_{ij}) = T_{ij} \otimes 1 + 1 \otimes T_{ij} + R_{ij}$$

where R_{ij} *is an element of* $k[G_{i-1}] \otimes_k k[G_{i-1}]$.

Proof. It is enough to prove the statement for $G = G_n$ and we set $r := r_n$. By Proposition 2.2.12, $G \subseteq (W_n)^s$ for some $s \geq 1$. We then have the following commutative diagram with vertical maps being closed immersions

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H_n & \longrightarrow & G & \longrightarrow & G_{n-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{G}_a^s & \longrightarrow & (W_n)^s & \xrightarrow{\pi} & (W_{n-1})^s & \longrightarrow & 0.
\end{array}$$

Now,

$$H_n = \mathrm{Im}(V_G^{n-1}) \simeq \prod_{j=1}^{r} \alpha_{p^{l_j}} \subseteq \mathbb{G}_a^r$$

for some $1 \leq r \leq s$ and $l_1, \ldots, l_r \geq 1$. By Lemma 2.2.24 there exists a projection

$$\rho \colon (W_n)^s \twoheadrightarrow (W_n)^r$$

such that the composite

$$H_n \hookrightarrow (W_n)^s \twoheadrightarrow (W_n)^r$$

is a monomorphism and thus $H_n \hookrightarrow \mathbb{G}_a^r$. Consider the commutative diagram given by the schematic images of ρ:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_n & \longrightarrow & \rho(G) & \longrightarrow & \rho(G_{n-1}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_a^r & \longrightarrow & (W_n)^r & \xrightarrow{\pi} & (W_{n-1})^r & \longrightarrow & 0. \end{array}$$

Its vertical maps are closed immersions and they factor in the following way

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_n & \longrightarrow & \rho(G) & \longrightarrow & \rho(G_{n-1}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_a^r & \longrightarrow & \pi^{-1}(\rho(G_{n-1})) & \xrightarrow{\pi} & \rho(G_{n-1}) & \longrightarrow & 0. \end{array} \tag{2.1}$$

Notice that $\pi^{-1}(\rho(G_{n-1})) = \rho(G_{n-1}) \times_k \mathbb{A}_k^r$ as k-schemes with structure of k-group scheme given by the embedding $\pi^{-1}(\rho(G_{n-1})) \hookrightarrow (W_n)^r$. In particular

$$k[\pi^{-1}(\rho(G_{n-1}))] = k[\rho(G_{n-1})][T_1, \ldots, T_r],$$

with comultiplication extending that of $k[\rho(G_{n-1})]$ and such that

$$\Delta(T_i) = T_i \otimes 1 + 1 \otimes T_i + R_i$$

where R_i is an element of $k[\rho(G_{n-1})] \otimes_k k[\rho(G_{n-1})]$. Since $\rho(G) \to \rho(G_{n-1})$ and $G \to G_{n-1}$ are both H_n-torsors and $G \to \rho(G)$ is H_n-equivariant, the commutative diagram

$$\begin{array}{ccc} G & \longrightarrow & G_{n-1} \\ \downarrow & & \downarrow \\ \rho(G) & \longrightarrow & \rho(G_{n-1}) \end{array}$$

is indeed a pull-back diagram. Therefore,

$$G = G_{n-1} \times_{\rho(G_{n-1})} \rho(G),$$

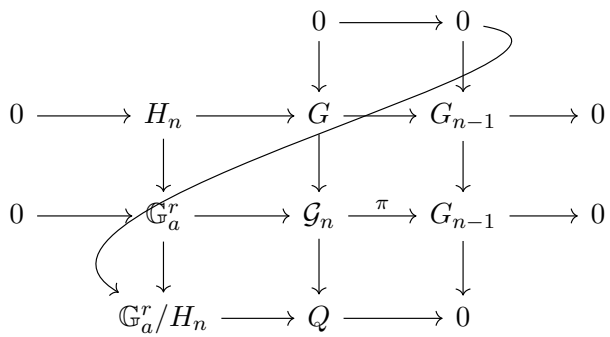
which is a closed subgroup scheme of $\mathcal{G}_n := G_{n-1} \times_{\rho(G_{n-1})} \pi^{-1}(\rho(G_{n-1}))$. Moreover

$$\begin{aligned} k[\mathcal{G}_n] &= k[G_{n-1}] \otimes_{k[\rho(G_{n-1})]} k[\pi^{-1}(\rho(G))] \\ &= k[G_{n-1}] \otimes_{k[\rho(G_{n-1})]} k[\rho(G_{n-1})][T_1, \ldots, T_r] \\ &= k[G_{n-1}][T_1, \ldots, T_r] \end{aligned}$$

with comultiplication extending that of $k[G_{n-1}]$ and such that

$$\Delta(T_i) = T_i \otimes 1 + 1 \otimes T_i + R_i$$

where R_i is an element of $k[G_{n-1}] \otimes_k k[G_{n-1}]$ as wished. Pulling back the exact sequences in (2.1) and by the Snake Lemma, we have a zig-zag map as in the following diagram:



which concludes the proof. □

Remark 2.2.31. Let us point out that the important result of the above Proposition is that the k-Hopf algebra structure of

$$k[\mathcal{G}_i] = k[G_{i-1}][T_{i1}, \ldots, T_{ir_i}]$$

extends that of $k[G_{i-1}]$ and is such that

$$\Delta(T_{ij}) = T_{ij} \otimes 1 + 1 \otimes T_{ij} + R_{ij}$$

where R_{ij} is an element of $k[G_{i-1}] \otimes_k k[G_{i-1}]$. We also translate here the above statement at the level of algebras, since it will be useful in the proof of Theorem 3.2.13. The short exact sequence

$$0 \to G_i \to \mathcal{G}_i \to \mathbb{G}_a^{r_i} \to 0$$

corresponds to

$$\begin{array}{c} 0 \to (S_1, \ldots, S_{r_i}) \to k[G_{i-1}][T_{i1}, \ldots, T_{ir_i}] \to k[G_i] \to 0 \\ S_i \mapsto P_i \end{array}$$

where $k[\mathbb{G}_a^{r_i}] = k[S_1, \ldots, S_{r_i}]$. Therefore

$$k[G_i] = k[G_{i-1}][T_{i1}, \ldots, T_{ir_i}]/(P_1, \ldots, P_{r_i})$$

where the polynomials P_j are primitive elements of $k[G_{i-1}][T_{i1}, \ldots, T_{ir_i}]$. Notice moreover that the polynomials P_j are congruent to $T_{ij}^{p^{l_{ij}}}$ for some $l_{ij} \geq 1$ modulo the augmentation ideal of $k[G_{i-1}]$ for every $j = 1, \ldots, r_i$ by the short exact sequence

$$\begin{array}{c} 0 \to I_{G_{i-1}} \to k[G_{i-1}][T_1, \ldots, T_{r_i}] \to k[T_1, \ldots, T_r] \to 0 \\ P_j \mapsto T_{ij}^{p^{l_{ij}}}. \end{array}$$

Example 2.2.32. Let us illustrate also via an example the proof of Proposition 2.2.30. Consider the k-group scheme $G = \alpha_p \times_k W_2^1$. Then V_G has nilpotency index 2 and $G \subseteq (W_2)^2$. We then have the commutative diagram with vertical maps being closed immersions

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_2 & \longrightarrow & G & \longrightarrow & G_1 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_a^2 & \longrightarrow & (W_2)^2 & \xrightarrow{\pi} & (W_1)^2 & \longrightarrow & 0 \end{array}$$

where

$$H_2 = \mathrm{Im}(V_G) \simeq \alpha_p \subseteq \mathbb{G}_a$$

and $G_1 \simeq \alpha_p \times_k \alpha_p$. Notice that H_2 is the copy of α_p contained in $W_2^1 \subseteq G$ given by the image of the Verschiebung (of W_2^1). As a consequence, the projection on the second factor

$$\rho\colon (W_2)^2 \twoheadrightarrow W_2$$

is such that the composite

$$H_2 \hookrightarrow (W_2)^2 \twoheadrightarrow W_2$$

is a monomorphism. Taking the schematic images of ρ we obtain the commutative diagram given by:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_2 & \longrightarrow & \rho(G) & \longrightarrow & \rho(G_1) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_a & \longrightarrow & W_2 & \xrightarrow{\pi} & W_1 & \longrightarrow & 0 \end{array}$$

where $\rho(G) = W_2^1$ and $\rho(G_1) \simeq \alpha_p$. Its vertical maps are closed immersions and they factor in the following way

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_2 & \longrightarrow & \rho(G) & \longrightarrow & \rho(G_1) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{G}_a & \longrightarrow & \pi^{-1}(\rho(G_1)) & \xrightarrow{\pi} & \rho(G_1) & \longrightarrow & 0. \end{array} \tag{2.2}$$

Notice that $\pi^{-1}(\rho(G_1)) = \rho(G_1) \times_k \mathbb{A}_k^1 \simeq \alpha_p \times_k \mathbb{A}_k^1$ as k-schemes with structure of k-group scheme given by the embedding $\pi^{-1}(\rho(G_1)) \hookrightarrow (W_2)^2$. In particular

$$k[\pi^{-1}(\rho(G_1))] = k[\rho(G_1)][T_1] = k[T_0]/(T_0^p)[T_1],$$

with comultiplication extending that of $k[\rho(G_1)]$ and such that

$$\Delta(T_1) = T_1 \otimes 1 + 1 \otimes T_1 + S_1(T_0 \otimes 1, 1 \otimes T_0).$$

Now, as in the proof, we have

$$G = G_1 \times_{\rho(G_1)} \rho(G),$$

which is a closed subgroup scheme of $\mathcal{G}_2 := G_1 \times_{\rho(G_1)} \pi^{-1}(\rho(G_1))$. Moreover

$$k[\mathcal{G}_2] = k[G_1] \otimes_{k[\rho(G_1)]} k[\pi^{-1}(\rho(G))]$$

$$= k[G_1] \otimes_{k[\rho(G_1)]} k[\rho(G_1)][T_1]$$
$$= k[G_1][T_1] = k[S_0, T_0]/(S_0^p, T_0^p)[T_1]$$

with comultiplication extending that of $k[G_1]$ and such that

$$\Delta(T_1) = T_1 \otimes 1 + 1 \otimes T_1 + S_1(T_0 \otimes 1, 1 \otimes T_0)$$

and

$$k[G] = (k[S_0, T_0]/(S_0^p, T_0^p))\,[T_1]/(T_1^p).$$

2.3 Infinitesimal commutative unipotent group schemes with one-dimensional Lie algebra

In general, it is not easy to describe explicitly infinitesimal commutative unipotent group schemes. For example, already those arising as the p-torsion of some abelian variety (with p-rank zero) are not completely understood and increase in complexity as the dimension grows. To have an explicit description of such group schemes, for example in terms of the Hopf algebra representing them, is useful in order to construct actions of these group schemes on varieties (see for example Proposition 3.1.17). In this section, we deal with this problem for the case of infinitesimal commutative unipotent group schemes with one-dimensional Lie algebra defined over an algebraically closed field k, proving the following result.

Theorem 2.3.1. *Let k be an algebraically closed field of characteristic $p > 0$. For any $n \geq 1$, there are exactly, up to isomorphism, n infinitesimal commutative unipotent k-group schemes of order p^n and with one-dimensional Lie algebra. They are the group schemes of the form*

$$W_n^n[V - F^i] := \ker(V - F^i \colon W_n^n \to W_n^n)$$

for some $i = 1, \ldots, n$.

This result is known for infinitesimal commutative unipotent group schemes of order $\leq p^3$ thanks to [Oor66, (15.5)] and [NWW15, Theorem 1.1].

We see that, of these group schemes, the only ones that are contained in a smooth connected one-dimensional algebraic group are α_{p^n} and $W_n^n[F - V]$ (the former is a subgroup of $\mathbb{G}_a$ and the latter is contained in the p^n-torsion of a supersingular elliptic curve) for any $n \geq 1$, see Proposition 2.3.12. All the others are examples of infinitesimal group schemes that act generically freely on any curve (by Theorem 3.2.13 in Chapter 3), but are not subgroups of a smooth connected one-dimensional algebraic group. We answer in this way to a question of Brion (see [Bri22]). Notice moreover that $W_n^n[F - V]$ is the only self-dual group scheme of the list. If one considers infinitesimal commutative unipotent group schemes with higher dimensional Lie algebra, this is not the case anymore: indeed the p-torsion of any principally polarized abelian variety of dimension g and p-rank

zero, is a self-dual infinitesimal commutative unipotent group scheme, and there exist p^{g-1} different isomorphism classes of such varieties (see [Pri08]).

The commutative group schemes of Theorem 2.3.1 are infinitesimal unipotent since their Frobenius and Verschiebung morphisms are both nilpotent (see Remark 2.2.13) and they have one-dimensional Lie algebra since for all of them the Frobenius kernel is α_p (see Remark 2.1.6). As recalled in Proposition 2.2.12, if the base field k is perfect, every infinitesimal commutative unipotent k-group scheme G can be embedded in $(W_n^m)^r$ for some $n, m, r \geq 1$. When either G or its Cartier dual has one-dimensional Lie algebra, then they both embed in just one copy of the group scheme of Witt vectors (Corollary 2.2.25), but this is not the only case as we see in Lemma 2.3.4. Until the end of 2.3 we will assume that k is a perfect field. Moreover W will denote the group scheme of Witt vectors over k, W_n the k-group scheme of Witt vectors of length $\leq n$ and W_n^m the kernel of the morphism $F^m \colon W_n \to W_n$.

In the following Lemma we compute the Hopf algebra representing certain infinitesimal commutative unipotent group schemes which will play a key role further on.

Lemma 2.3.2. *For every integer $r, s \geq 1$ and $m \geq 2$ let $d = lcm(r, s)$ and consider the k-group scheme $G = W_{md}^{md}[F^r - V^s]$. Then*

(i) $G = W_n^{n'}[F^r - V^s]$ where $n = \min\left(sm\frac{d}{r}, md\right)$ and $n' = \min\left(rm\frac{d}{s}, md\right)$, and

(ii) the k-Hopf algebra of G is

$$k[G] = k[T_0, \ldots, T_{n-1}]/(T_0^{p^r}, \ldots, T_{s-1}^{p^r}, T_s^{p^r} - T_0, \ldots, T_{n-1}^{p^r} - T_{n-s-1})$$

where $k[T_0, \ldots, T_{n-1}]$ is the k-Hopf algebra $k[W_n]$ of Witt vectors of length $\leq n$, that is the comultiplication on $k[G]$ is given by that of Witt vectors.

Proof. For the first statement, the inclusion $W_n^{n'}[F^r - V^s] \subseteq G$ is clear since $n, n' \leq md$. For the other inclusion, notice that $s \mid n$ and $r \mid n'$ and thus

$$V_G^n = (V_G^s)^{\frac{n}{s}} = (F_G^r)^{\frac{n}{s}} = 0 \quad \text{and} \quad F_G^{n'} = (F_G^r)^{\frac{n'}{r}} = (V_G^s)^{\frac{n'}{r}} = 0.$$

For the second statement, notice that for any k-algebra R we have

$$G(R) =$$

$$\left\{\underline{a} \in W_n(R) \mid \left(a_0^{p^r}, \ldots, a_{s-1}^{p^r}, a_s^{p^r}, \ldots, a_{n-1}^{p^r}\right) = (0, \ldots, 0, a_0, \ldots, a_{n-s-1}) \text{ and } a_i^{p^{n'}} = 0 \ \forall i\right\}$$

$$= \left\{\underline{a} \in W_n(R) \mid \left(a_0^{p^r}, \ldots, a_{s-1}^{p^r}, a_s^{p^r} - a_0, \ldots, a_{n-1}^{p^r} - a_{n-s-1}\right) = \underline{0} \text{ and } a_i^{p^{n'}} = 0 \ \forall i\right\}$$

$$= \left\{\underline{a} \in W_n(R) \mid \left(a_0^{p^r}, \ldots, a_{s-1}^{p^r}, a_s^{p^r} - a_0, \ldots, a_{n-1}^{p^r} - a_{n-s-1}\right) = \underline{0}\right\}$$

where $\underline{a} = (a_0, \ldots, a_{n-1})$ and the last equality is due to the fact that $n' \geq 2r$: indeed clearly $a_i^{p^{n'}} = 0$ for every $i = 0, \ldots, s-1$ since in this case $a_i^{p^r} = 0$ and for $i = s, \ldots, n-1$ we have $a_i^{p^{n'}} = a_{i-s}^{p^{n'-r}} = 0$. □

Example 2.3.3. Notice that in general it is slightly more difficult to write explicitly the Hopf algebra representing the group scheme $W_n^n[F^r - V^s]$ for any $n \geq 1$ and $r, s = 1, \ldots, n$. Take for example

$$G = W_3^3[V - F^2] = W_2^3[V - F^2].$$

Notice that $G = \ker(F_H^3)$ where $H = W_4^4[V - F^2] = W_2^4[V - F^2] = \mathrm{Spec}(A)$ and

$$A = k[T_0, T_1]/(T_0^{p^2}, T_1^{p^2} - T_0)$$

by Lemma 2.3.2. Therefore,

$$k[G] = A/(T_0^{p^3}, T_1^{p^3}) = k[T_0, T_1]/(T_0^{p^2}, T_1^{p^2} - T_0, T_0^{p^3}, T_1^{p^3}) = k[T_0, T_1]/(T_0^p, T_1^{p^2} - T_0).$$

In the following we see that there are many examples of infinitesimal commutative unipotent group schemes G that embed in just one copy of the group scheme of Witt vectors but neither G nor $G^\vee$ have one-dimensional Lie algebra.

Lemma 2.3.4. *For every integer $r, s \geq 1$ and $m \geq 2$ let $d = lcm(r, s)$, $n = \min\left(sm\frac{d}{r}, md\right)$ and $n' = \min\left(rm\frac{d}{s}, md\right)$. The Dieudonné module of the k-group scheme*

$$G = W_{md}^{md}[F^r - V^s] = W_n^{n'}[F^r - V^s]$$

is

$$M(G) = E/(E(\mathbb{F}^r - \mathbb{V}^s) + E\mathbb{F}^{n'}).$$

Moreover, the Cartier dual of G is

$$G^\vee = W_{n'}^n[V^r - F^s].$$

Proof. Set $E_n^{n'} := M(W_n^{n'}) = E/(E\mathbb{F}^{n'} + E\mathbb{V}^n)$. The short exact sequence

$$0 \to G \to W_n^{n'} \to \mathrm{Im}(F^r - V^s) \to 0$$

yields the short exact sequence of E-modules

$$0 \to E_n^{n'}(\mathbb{F}^r - \mathbb{V}^s) \to E_n^{n'} \to M(G) \to 0$$

and thus $M(G) = E/(E(\mathbb{F}^r - \mathbb{V}^s) + E\mathbb{F}^{n'})$ as stated. Consider now the Cartier dual $G^\vee$ of G. First of all, let us show that $G^\vee$ embeds in just one copy of the k-group scheme of Witt vectors. Indeed, if this was not the case, by Corollary 2.2.24, $G^\vee$ would contain $\alpha_p \times_k \alpha_p$ as a k-subgroup scheme. As a consequence, we would have a surjection

$$G \twoheadrightarrow \alpha_p \times_k \alpha_p,$$

implying that $k[\alpha_p \times_k \alpha_p] = k[U_1, U_2]/(U_1^p, U_2^p)$ is a k-Hopf subalgebra of $k[G]$. This is not the case since there exists a unique, up to scalar multiplication, element $x \in k[G]$ such that $\Delta(x) = x \otimes 1 + 1 \otimes x$ and $x^p = 0$ (this element is $T_0^{p^{r-1}}$ with the notation of the description of $k[G]$ given in Lemma 2.3.2), while $k[\alpha_p \times_k \alpha_p]$ has two k-linearly independent elements

with this property. Therefore $G^\vee \subseteq W_{n'}^n$. Moreover, $V^r_{(G^\vee)^{(1/p)}} - F^s_{G^\vee} = (F^r_G - V^s_{G^{(1/p)}})^\vee = 0$ and thus

$$G^\vee \subseteq W_{n'}^n[V^r - F^s].$$

By Lemma 2.3.2,

$$o\left(W_{n'}^n[V^r - F^s]\right) = p^{sn'} = p^{rn} = o(G) = o(G^\vee),$$

hence the equality. □

Example 2.3.5. Notice that in general it is not true that an infinitesimal commutative unipotent k-group scheme and its Cartier dual are contained in the same (minimal) number of copies of Witt vectors. Consider for example the k-subgroup scheme of $W_2 \times_k W_2$ given by

$$G = \operatorname{Spec}\left(k[T_0, T_1, U_0, U_1]/(T_0^p, T_1^p - U_0, U_0^p, U_1^p - T_0)\right)$$

and the quotient

$$G \twoheadrightarrow H = \operatorname{Spec}\left(k[T_0, T_1, U_0]/(T_0^p, T_1^p - U_0, U_0^p)\right) \simeq \operatorname{Spec}\left(k[T_0, T_1]/(T_0^p, T_1^{p^2})\right).$$

Then H is a k-subgroup scheme of W_2 but its dual is not. Indeed, one can see that G is self-dual setting $\widetilde{T}_0 = T_1^*, \widetilde{T}_1 = U_0^*, \widetilde{U}_0 = U_1^*, \widetilde{U}_1 = T_0^*$ and, as a consequence, we have

$$H^\vee = \operatorname{Spec}\left(k[\widetilde{T}_0, \widetilde{T}_1, \widetilde{U}_1]/(\widetilde{T}_0^p, \widetilde{T}_1^p, \widetilde{U}_1^p - \widetilde{T}_0)\right) \simeq \operatorname{Spec}\left(k[X, Y]/(X^{p^2}, Y^p)\right)$$

with comultiplication

$$\begin{aligned}\Delta\colon X &\mapsto X \otimes 1 + 1 \otimes X,\\ Y &\mapsto Y \otimes 1 + 1 \otimes Y + S_1(X^p, X^p)\end{aligned}$$

where $S_1(a, b) = -\sum_{k=1}^p \frac{1}{p}\binom{p}{k} a^k b^{p-k}$. We also remark that $\ker(F_H) \simeq W_2^1$, while $\ker(F_{H^\vee}) \simeq \alpha_p \times_k \alpha_p$. One can show that indeed G is isomorphic to

$$\ker(F - V\colon W_2 \to W_2)^2 = \operatorname{Spec}\left(k[X_0, X_1, Y_0, Y_1]/(X_0^p, X_1^p - X_0, Y_0^p, Y_1^p - Y_0)\right).$$

The isomorphism is explicitly given by

$$\begin{aligned}X_0 &\mapsto T_0 + U_0,\\ X_1 &\mapsto T_1 + U_1 + S_1(T_0, U_0),\\ Y_1 &\mapsto -T_1 + U_1 + S_1(T_0, -U_0),\\ Y_0 &\mapsto T_0 - U_0.\end{aligned}$$

As shown later on (see Corollary 2.3.10), over an algebraically closed field, this is the product of two copies of the p-torsion of a supersingular elliptic curve over k.

Lemma 2.3.6. *Let G be an infinitesimal commutative unipotent k-group scheme of order p^n with one-dimensional Lie algebra. Then, up to (canonical) isomorphism, the Dieudonné module of $\ker(F_G^{n-1})$ is given by the quotient $M(G)/M(G)\mathbb{F}^{n-1}$.*

Proof. We start by remarking that, by Lemma 2.2.10, G has height n. Moreover, by Theorem 2.1.9, $G \simeq \mathrm{Spec}(k[T]/(T^{p^n}))$ as schemes and thus

$$F_G^{n-1}(G) \simeq \mathrm{Spec}(k[T^{p^{n-1}}]/(T^{p^n})) \simeq \mathrm{Spec}(k[U]/(U^p)).$$

Since $F_G^{n-1}(G)$ is still unipotent, then $F_G^{n-1}(G) \simeq \alpha_p$. Therefore, we have the short exact sequence

$$0 \longrightarrow H \longrightarrow G \xrightarrow{F_G^{n-1}} \alpha_p \longrightarrow 0$$

where $H := \ker(F_G^{n-1})$. Applying the (exact contravariant) Dieudonné functor we obtain the short exact sequence

$$0 \longrightarrow M(\alpha_p) \xrightarrow{M(F_G^{n-1})} M(G) \longrightarrow M(H) \longrightarrow 0.$$

Now, $\mathbb{F}^{n-1}$ is zero in $M(H)$ and thus we have the factorization

$$M(G)/M(G)\mathbb{F}^{n-1} \twoheadrightarrow M(H).$$

Therefore $M(G)\mathbb{F}^{n-1}$ is contained in the kernel of $M(G) \to M(H)$ that is (isomorphic to) $M(\alpha_p)$. Finally, since $M(G)\mathbb{F}^{n-1} \neq 0$ and $M(\alpha_p)$ has length one, then also $M(G)\mathbb{F}^{n-1}$ has length one (and $M(G)\mathbb{F}^{n-1} \simeq M(\alpha_p)$). Therefore $M(G)/M(G)\mathbb{F}^{n-1}$ is isomorphic to $M(H)$. □

Proposition 2.3.7. *Let k be algebraically closed and $n \geq 3$. Then for every $a \in W(k)$ and $i = 1, \ldots, n-2$ we have an isomorphism of E-modules*

$$E/\left(E(\mathbb{V} - \mathbb{F}^i - a\mathbb{F}^{n-1}) + E\mathbb{F}^n\right) \simeq E/\left(E(\mathbb{V} - \mathbb{F}^i) + E\mathbb{F}^n\right).$$

Moreover, for every $a \in W(k)^\times$ it holds

$$E/\left(E(\mathbb{V} - a\mathbb{F}^{n-1}) + E\mathbb{F}^n\right) \simeq E/\left(E(\mathbb{V} - \mathbb{F}^{n-1}) + E\mathbb{F}^n\right)$$

as E-modules.

Proof. We will show that for any $i = 1, \ldots, n-2$

$$\begin{aligned} \varphi\colon E/\left(E(\mathbb{V} - \mathbb{F}^i - a\mathbb{F}^{n-1}) + E\mathbb{F}^n\right) &\to E/\left(E(\mathbb{V} - \mathbb{F}^i) + E\mathbb{F}^n\right) \\ 1 &\mapsto 1 + c\mathbb{F}^{n-1-i} \end{aligned}$$

is an isomorphism for a good choice of $c \in W(k)$. First, we have to find under what conditions on c is φ well-defined. This is the case if and only if $\varphi(\mathbb{V} - \mathbb{F}^i - a\mathbb{F}^{n-1}) = 0$. Now

$$\varphi(\mathbb{V} - \mathbb{F}^i - a\mathbb{F}^{n-1}) = (\mathbb{V} - \mathbb{F}^i - a\mathbb{F}^{n-1})(1 + c\mathbb{F}^{n-1-i}) =$$

$$\mathbb{V} - \mathbb{F}^i - a\mathbb{F}^{n-1} + (\mathbb{V} - \mathbb{F}^i - a\mathbb{F}^{n-1})c\mathbb{F}^{n-1-i} = -a\mathbb{F}^{n-1} + \sigma^{-1}(c)\mathbb{V}\mathbb{F}^{n-1-i} - \sigma^i(c)\mathbb{F}^{n-1} =$$

$$-a\mathbb{F}^{n-1} + \sigma^{-1}(c)\mathbb{F}^{n-1} - \sigma^i(c)\mathbb{F}^{n-1} = (-a + \sigma^{-1}(c) - \sigma^i(c))\mathbb{F}^{n-1}$$

where σ is the Frobenius morphism on $W(k)$. Let us note $\gamma := -a + \sigma^{-1}(c) - \sigma^i(c)$. Since $\mathbb{F}^n = 0$, it is enough to find c such that $\gamma = 0 \mod p$. We take $c = [c_0]$ to be the Teichmüller lift of a non-zero solution c_0 of the polynomial $X - X^{p^{i+1}} = a_0^p$, which exists since k is algebraically closed. Therefore, the morphism φ is well-defined. Let us show that φ is injective. Since in the source of φ we have $\mathbb{V} = \mathbb{F}^i + a\mathbb{F}^{n-1}$, a general element of the source is of the form $\sum_{k=0}^{n-1} a_k \mathbb{F}^k$ with $a_k \in W(k)$. Moreover, since k is perfect, for any $\alpha = (\alpha_0, \alpha_1, \dots) \in W(k)$ we have

$$\alpha = [\alpha_0] + (0, \alpha_1, \alpha_2, \dots) = [\alpha_0] + p\left(\alpha_1^{1/p}, \alpha_2^{1/p}, \dots\right) = [\alpha_0] + \left(\alpha_1^{1/p}, \alpha_2^{1/p}, \dots\right) p$$

and thus

$$\alpha\mathbb{F}^k = [\alpha_0]\mathbb{F}^k + \left(\alpha_1^{1/p}, \alpha_2^{1/p}, \dots\right) \mathbb{V}\mathbb{F}^{k+1} = [\alpha_0]\mathbb{F}^k + \left(\alpha_1^{1/p}, \alpha_2^{1/p}, \dots\right) \mathbb{F}^{k+1+i}.$$

Since $\mathbb{F}^n = 0$, repeating the argument for $\left(\alpha_1^{1/p}, \alpha_2^{1/p}, \dots\right) \mathbb{F}^{k+1+i}$ we obtain that for a general element $\sum_{k=0}^{n-1} a_k \mathbb{F}^k$ in the quotient we can suppose that a_k is the Teichmüller lift of some element of the base field for any $k = 0, \dots, n-1$. Suppose now that such an element maps to zero. Then we have

$$0 = \left(\sum_{k=0}^{n-1} a_k \mathbb{F}^k\right)(1 + c\mathbb{F}^{n-1-i}) = \sum_{k=0}^{n-1} a_k \mathbb{F}^k + \sum_{k=0}^{n-1} a_k \mathbb{F}^k c \mathbb{F}^{n-1-i} =$$

$$\sum_{k=0}^{n-1} a_k \mathbb{F}^k + \sum_{k=0}^{n-1} a_k \sigma^k(c) \mathbb{F}^{n-1-i+k} = \sum_{k=0}^{n-1} a_k \mathbb{F}^k + \sum_{k=0}^{i} a_k \sigma^k(c) \mathbb{F}^{n-1-i+k}$$

that is

$$\sum_{k=0}^{n-1} a_k \mathbb{F}^k = -\sum_{k=0}^{i} a_k \sigma^k(c) \mathbb{F}^{n-1-i+k}.$$

Multiplying recursively on the right by $\mathbb{F}^{n-j}$ for $j = 1, \dots, n-1$ one obtains $a_k \mathbb{F}^{n-1} = 0$ and since a_k is a Teichmüller lift, this implies that $a_k = 0$ for all $k = 0, \dots, n-1$. Therefore φ is injective and since both the E-modules $E/\left(E(\mathbb{V} - \mathbb{F}^i - a\mathbb{F}^{n-1}) + E\mathbb{F}^n\right)$ and $E/\left(E(\mathbb{V} - \mathbb{F}^i) + E\mathbb{F}^n\right)$ have length n then φ is an isomorphism. Let us conclude the proof showing that

$$E/\left(E(\mathbb{V} - a\mathbb{F}^{n-1}) + E\mathbb{F}^n\right) \simeq E/\left(E(\mathbb{V} - \mathbb{F}^{n-1}) + E\mathbb{F}^n\right)$$

when $a \in W(k)^\times$. Notice that in both E-modules we have $p = \mathbb{F}\mathbb{V} = \mathbb{V}\mathbb{F} = 0$ since $\mathbb{F}^n = 0$ and $\mathbb{V} = a\mathbb{F}^{n-1}$ or $\mathbb{V} = \mathbb{F}^{n-1}$. We can then suppose that $a = [\overline{a}]$ is the Teichmüller lift of some element $\overline{a} \in k$. We define the morphism ψ sending 1 to the Teichmüller lift $b = [\overline{b}]$ of a non-zero root $\overline{b}$ of the polynomial $\overline{a}^p X^{p^n} - X$, which exists since k is algebraically closed. Remark that ψ is well-defined since

$$\mathbb{V} - a\mathbb{F}^{n-1} \mapsto (\mathbb{V} - a\mathbb{F}^{n-1})b = \sigma^{-1}(b)\mathbb{V} - a\sigma^{n-1}(b)\mathbb{F}^{n-1} = (\sigma^{-1}(b) - a\sigma^{n-1}(b))\mathbb{F}^{n-1} = 0.$$

In fact, once more $\mathbb{V}\mathbb{F}^{n-1} = 0$ and thus it is enough to verify that $\delta_0 = 0$ where $\delta := \sigma^{-1}(b) - a\sigma^{n-1}(b)$, which holds true since

$$\delta_0 = \left(\overline{b} - \overline{a}^p \overline{b}^{p^n}\right)^{1/p} = 0.$$

Finally, ψ is surjective, since

$$b^{-1} = \left[\overline{b}^{-1}\right] \mapsto 1$$

and thus an isomorphism. □

We are now ready to prove Theorem 2.3.1.

Proof of Theorem 2.3.1. We argue by induction on n. For $n = 1$ the only infinitesimal commutative unipotent group scheme of order p with one-dimensional Lie algebra is α_p and its Dieudonné module is $E/(E\mathbb{V} + E\mathbb{F})$. Suppose now that the statement is true for $n-1$ and let G be an infinitesimal commutative unipotent k-group scheme of order p^n and one-dimensional Lie algebra. Consider then the short exact sequence

$$0 \to \ker(F_G^{n-1}) \to G \to F_G^{n-1}(G) \simeq \alpha_p \to 0.$$

Then $\ker(F_G^{n-1})$ is a subgroup scheme of G of order p^{n-1} so by inductive hypothesis

$$\ker(F_G^{n-1}) = W_{n-1}^{n-1}[V - F^i]$$

for some $i = 1, \dots, n-1$. Equivalently we have a surjection

$$M(G) \twoheadrightarrow M(G)/M(G)\mathbb{F}^{n-1} \simeq E/\left(E(\mathbb{V} - \mathbb{F}^i) + E\mathbb{F}^{n-1}\right) \tag{2.3}$$

where $M(G)$ is the Dieudonné module corresponding to G and we know that $M(G)$ is an E-module of length n (the isomorphism is given by Lemma 2.3.6). The kernel of this surjection is thus $M(G)\mathbb{F}^{n-1} = k\mathbb{F}^{n-1}$, where the equality is due to the fact that $\mathbb{F}^n = 0$. Therefore, by (2.3), it holds $\mathbb{V} - \mathbb{F}^i = a\mathbb{F}^{n-1}$ in $M(G)$ for some $a \in W(k)$ (and we can take $a = [\overline{a}]$ for some $\overline{a} \in k$). As a consequence we have the surjection

$$E/(E\mathbb{V}^n + E\mathbb{F}^n) \twoheadrightarrow M(G)$$

coming from the fact that $G \subseteq W_n^n$ (by Corollary 2.2.25) factors via

$$E/\left(E(\mathbb{V} - \mathbb{F}^i - a\mathbb{F}^{n-1}) + E\mathbb{F}^n\right) \twoheadrightarrow M(G).$$

Finally, both the E-modules $M(G)$ and $E/\left(E(\mathbb{V} - \mathbb{F}^i - a\mathbb{F}^{n-1}) + E\mathbb{F}^n\right)$ have length n and thus

$$M(G) \simeq E/\left(E(\mathbb{V} - \mathbb{F}^i - a\mathbb{F}^{n-1}) + E\mathbb{F}^n\right).$$

The statement follows by Proposition 2.3.7. □

Remark 2.3.8. Notice that as a consequence of the proof of Theorem 2.3.1 we have that, for $i = 1, \dots, n-2$, $W_n^n[V - F^i]$ is the only infinitesimal commutative unipotent group scheme of order p^n and with one-dimensional Lie algebra that is an extension of α_p by $W_{n-1}^{n-1}[V - F^i]$. On the other hand, there are exactly two infinitesimal commutative unipotent group schemes of order p^n and with one-dimensional Lie algebra that are an extension of α_p by $\alpha_{p^{n-1}}$: $W_n^n[V - F^{n-1}]$ and α_{p^n}.

As direct consequences of Theorem 2.3.1 and Lemma 2.3.4 we have the following two corollaries, that respectively describe (over algebraically closed fields) all infinitesimal commutative unipotent k-group schemes whose dual have one-dimensional Lie algebra, and the p^n-torsion of supersingular elliptic curves. The latter is probably well-known, but we are not aware of a reference for it.

Corollary 2.3.9. *Let k be algebraically closed. For any $n \geq 1$, there are exactly n non-isomorphic infinitesimal commutative unipotent k-group schemes G of order p^n such that $\dim_k(\mathrm{Lie}(G^\vee)) = 1$. They are the group schemes of the form*

$$W_n^n[F - V^i] := \ker(F - V^i \colon W_n^n \to W_n^n)$$

for some $i = 1, \dots, n$.

Proof. The classification is a direct consequence of Theorem 2.3.1 along with Lemma 2.3.4. □

Corollary 2.3.10. *Let k be algebraically closed and E/k be a supersingular elliptic curve. Then, for every $n \geq 1$ its p^n-torsion is $E[p^n] = W_{2n}^{2n}[V - F]$.*

Proof. The p^n-torsion $E[p^n]$ of a supersingular elliptic curve E over an algebraically closed field of characteristic $p > 0$ is a finite commutative unipotent (see [Sil09, Theorem 3.1]) self-dual (see [Mum08, III.15, Theorem 1]) k-group scheme of order p^{2n} with one-dimensional Lie algebra. By Theorem 2.3.1 and Lemma 2.3.4, the only such k-group scheme is $W_{2n}^{2n}[F - V]$. □

Notice that if an infinitesimal commutative unipotent k-group scheme G with n-dimensional Lie algebra can be embedded in a smooth connected n-dimensional algebraic group $\mathcal{G}$, then G acts freely on it (by multiplication). Brion [Bri22, §1] asked if there are examples of generically free rational actions on curves of infinitesimal commutative unipotent group schemes that are not subgroup schemes of a smooth connected one-dimensional algebraic group. Recall that if $\mathcal{G}$ is a smooth connected one-dimensional k-algebraic group, then either $\mathcal{G}$ is affine and $\mathcal{G}_{\overline{k}} \simeq \mathbb{G}_{m,\overline{k}}$ or $\mathcal{G}_{\overline{k}} \simeq \mathbb{G}_{a,\overline{k}}$ or $\mathcal{G}$ is an elliptic curve. The following proposition explains that if k is algebraically closed, very few infinitesimal commutative unipotent k-group schemes with one-dimensional Lie algebra are contained in smooth connected one-dimensional algebraic groups. All the others are examples of infinitesimal group schemes that act generically freely on any curve (by Theorem 3.2.13 in Chapter 3), but are not subgroup schemes of a smooth connected algebraic group.

We need a small preliminary lemma.

Lemma 2.3.11. *Let $n > 2$ be an integer then $\frac{n}{2} > \lceil \frac{n}{3} \rceil$.*

Proof. For every real number x we have

$$x \leq \lceil x \rceil < x + 1.$$

It is then enough to show that $\frac{n}{2} \geq \frac{n}{3} + 1$. This holds if and only if $n \geq 6$. One can check by hand that for $n = 3, 4, 5$ the statement holds true as well. □

Proposition 2.3.12. *Let k be algebraically closed and G be an infinitesimal commutative unipotent k-group scheme with one-dimensional Lie algebra. Then G is contained in a smooth connected one-dimensional algebraic group if and only if either $G \simeq \alpha_{p^n}$ for some $n \geq 1$ (in this case $G \subseteq \mathbb{G}_a$) or $G \simeq W_n^n[V - F]$ (in this case G is contained in the p^n-torsion $E[p^n] = W_{2n}^{2n}[V - F]$ of a supersingular elliptic curve E).*

Proof. By Theorem 2.3.1, $G \simeq W_n^n[V - F^i]$ for some $n \geq 1$ and $i = 1, \ldots, n$. Let us start by considering the cases $i = 1, n$ for any $n \geq 1$. For $i = 1$ we have $G \simeq W_n^n[F - V]$ which is contained in $W_{2n}^{2n}[F - V]$ and the latter is the p^n-torsion of a supersingular elliptic curve (Corollary 2.3.10). For $i = n$, then $G \simeq W_1^n = \alpha_{p^n} \subseteq \mathbb{G}_a$.

Let us show that if $n > 2$ and $i = 2, \ldots, n - 1$ then G is not contained in a smooth connected one-dimensional algebraic group. Under these assumptions, clearly G is not a subgroup neither of $\mathbb{G}_m$ (since G is unipotent) nor of $\mathbb{G}_a$ (since $V_G \neq 0$). Therefore if G is a subgroup of a smooth connected one-dimensional algebraic group then it is a subgroup of an elliptic curve E. Notice that $p = V_G F_G = F_G^i F_G = F_G^{i+1}$ and thus $p^s = 0$ for $s = \lceil \frac{n}{i+1} \rceil$. Then, G is contained in the p^s-torsion $E[p^s]$ of E. Since $n > 2$ and $i + 1 \geq 3$, by Lemma 2.3.11 we have $\frac{n}{2} > s$. This gives a contradiction since $E[p^s]$ has order p^{2s} (see for example [Mum08] page 137) while G has order p^n with $n > 2s$. □

The question arises if all infinitesimal unipotent group schemes with one-dimensional Lie algebra are commutative (see both [Fak20, Remark 2.10] and [Bri22, §1]). The following example shows that it is not the case.

Example 2.3.13. Consider the infinitesimal unipotent non-commutative k-group scheme $G = \mathrm{Spec}(A)$ where

$$A = k[T_0, T_1] / \left(T_0^{p^n}, T_1^p - T_0 \right)$$

with $n \geq 2$ an integer and comultiplication given by

$$\Delta(T_0) = T_0 \otimes 1 + 1 \otimes T_0$$

and

$$\Delta(T_1) = T_1 \otimes 1 + 1 \otimes T_1 + T_0^{p^{n-1}} \otimes T_0^{p^{n-2}}.$$

In this case

$$A^\vee =$$

$$k\langle U_0 \ldots, U_n \rangle / (U_0^p, \ldots, U_n^p, U_i U_j - U_j U_i, U_n U_{n-1} - U_{n-1} U_n - U_0)_{i,j=0,\ldots n,(i,j),(j,i) \neq (n,n-1)}$$

where $U_0(T_1) = 1$ and $U_i(T_0^{p^{i-1}}) = 1$ and zero elsewhere. The Hopf algebra $A^\vee$ is non-commutative: the only non-commutative relation is given by $U_nU_{n-1} - U_{n-1}U_n = U_0$, while its comultiplication is defined on the U_i's as for the Witt vectors (notice that this makes sense since $U_0, \ldots, U_{n-1}$ commute). These examples arise as closed subgroup schemes of non-commutative extensions of $\mathbb{G}_a$ by itself (see [DG70, II.§3, 4]) and there are many of them. Other examples can be found in Section 3.4 of Chapter 3. In particular G is a subgroup scheme of $\mathrm{PGL}_{2,k}$ when k has characteristic 2 and $n = 3$ (see Theorem 3.4.1).

Chapter 3

Infinitesimal rational actions

The content of this chapter comes entirely from [Gou23] and [GT24].

Section 3.1 is devoted to generalities on (rational) actions of finite group schemes on varieties and their algebraic counterpart given by module algebra structures, introduced already in Chapter 1 (as background references we refer to [Mil17], [DG70], [SGA3], [Swe69], [Mon93]).

Section 3.2 deals with generically free rational actions of infinitesimal group schemes and contains one of the main results of this thesis (Theorem 3.2.13): in the first part of the section we prove the existence part of Theorem 3.2.13 in the case of commutative trigonalizable group schemes of height one (Proposition 3.2.4). We then proceed with the proof of the general case. We end the section with some examples to show more concretely how to deal with the construction of these actions.

Section 3.3 is devoted to Dolgachev's conjecture revisited for infinitesimal group schemes and, more generally, to studying faithful rational actions of infinitesimal group schemes. Dolgachev's conjecture [Dol10, Conjecture 37] can be rephrased in the following way: if there exists a faithful rational action of a finite commutative p-group G on $\mathbb{P}^n_k$ then $p_G^n = 0$, where p_G is the multiplication by p morphism on G. Proposition 3.3.6 gives necessary (but not sufficient, see the counterexample 3.3.7) conditions for the existence of faithful rational actions of infinitesimal commutative trigonalizable group schemes. Moreover, we show that for any infinitesimal commutative unipotent group scheme G defined over a perfect field and any variety X of dimension n, if $V_G^n = 0$ there exist faithful rational G-actions on X (Proposition 3.3.10).

Section 3.4 has as content the work [GT24], joint with Dajano Tossici, where unexpected subgroup schemes of $\mathrm{PGL}_{2,k}$ in characteristic 2 are studied. For any field k, $\mathrm{PGL}_{2,k}$ represents the automorphism group functor of $\mathbb{P}^1_k$ and thus subgroup schemes of $\mathrm{PGL}_{2,k}$ correspond to faithful actions on $\mathbb{P}^1_k$. Moreover, $\mathrm{PGL}_{2,k}(k)$ coincides with the Cremona group in dimension one, i.e. birational self-maps of $\mathbb{P}^1_k$, since any rational self-map of a projective non-singular curve extends to the whole curve. In positive characteristic, the situation is completely different if we consider rational actions of infinitesimal group schemes. Most of the faithful infinitesimal actions on the affine line do not extend to $\mathbb{P}^1_k$. If the characteristic of a field k is odd any infinitesimal group scheme of $\mathrm{PGL}_{2,k}$

lifts to $\mathrm{SL}_{2,k}$. We prove that this is not true in characteristic 2 and we give a complete description, up to isomorphism, of infinitesimal unipotent subgroup schemes of $\mathrm{PGL}_{2,k}$. Also, the infinitesimal trigonalizable case is considered.

3.1 Actions of finite group schemes

The first part of this section is devoted to recalling the main definitions around (rational) actions of finite group schemes on varieties, with a focus on faithful and (generically) free actions. The second part is centered on their algebraic counterpart which is given by module algebra structures (see Definition 1.1.13).

Actions and rational actions

Let G be a k-group scheme, X be a k-scheme equipped with a G-action $G \times_k X \to X$ and $\rho\colon G \to \mathrm{Aut}_X$ be the corresponding group functor homomorphism.

Definition 3.1.1 (Centralizer)**.** For any closed k-subscheme Y of X, the *centralizer* $C_G(Y)$ of Y in G is the subgroup functor that associates to any k-scheme S the set of $g \in G(S)$ inducing the identity on the S-scheme $Y \times_k S$. The kernel of ρ is the centralizer $C_G(X)$ of X in G.

Definition 3.1.2 (Faithful action)**.** Let G be a k-group scheme and X be a k-scheme equipped with a G-action $\rho\colon G \to \mathrm{Aut}_X$. The G-action is said to be *faithful* if its kernel is trivial.

Theorem 3.1.3. *Let G be a k-group scheme acting on a k-variety X. The centralizer $C_G(Y)$ of any closed k-subscheme Y of X is represented by a closed k-subgroup scheme of G.*

Proof. See [SGA3, $\mathrm{VI_B}$, Example 6.2.4.e)]. □

Lemma 3.1.4. *Let G be a k-group scheme and X be a k-variety endowed with a G-action. The G-action is faithful if and only if the induced $G_{\overline{k}}$-action on $X_{\overline{k}}$ is faithful.*

Proof. The $G_{\overline{k}}$-action on $X_{\overline{k}}$ is faithful if and only if $C_{G_{\overline{k}}}(X_{\overline{k}}) \simeq C_G(X)_{\overline{k}}$ is trivial and this holds true if and only if $C_G(X)$ is trivial. □

Definition 3.1.5 (Free action)**.** Let G be a finite k-group scheme and X be a k-scheme equipped with a G-action $\rho\colon G \times_k X \to X$. Let $x\colon \mathrm{Spec}(k(x)) \to X$ be a point of X and consider the composite $\psi : G \times_k \mathrm{Spec}(k(x)) \xrightarrow{\mathrm{id}\times x} G \times_k X \xrightarrow{\rho\times\mathrm{id}} X \times_k X$. The *stabilizer* $\mathrm{Stab}_G(x)$ of the point x is the pull-back of the diagram

$$\begin{array}{ccc} \mathrm{Stab}_G(x) & \dashrightarrow & G_{k(x)} \\ \vdots & & \downarrow{\scriptstyle \psi} \\ \mathrm{Spec}(k(x)) & \xrightarrow{diag} & X \times_k X \end{array}$$

where the bottom arrow is the diagonal morphism. The G-action is said to be *free at* $x \in X$ if $\mathrm{Stab}_G(x)$ is trivial. The G-action is said to be *free* if it is free at any point. We denote by X_{fr} the subset of free points of X, which is an open G-stable subset of X.

Remark 3.1.6. Notice that, by universal property of pull-backs, if H is a k-subgroup scheme of G, then

$$\mathrm{Stab}_H(x) = \mathrm{Stab}_G(x) \times_{G_{k(x)}} H_{k(x)}.$$

Proposition 3.1.7. *Let G be a finite k-group scheme and X be an irreducible k-scheme with a G-action. The following are equivalent:*

1. *$X_{fr} \neq \emptyset$;*
2. *the generic point η of X belongs to X_{fr};*
3. *X_{fr} is dense in X.*

Proof. As we recalled above, X_{fr} is an open G-stable subset of X. The statement is a direct consequence of this and of the fact that X is irreducible. □

Definition 3.1.8 (Generically free action)**.** Let G be a finite k-group scheme and X be an irreducible k-scheme with a G-action. We say that the action is *generically free* if it satisfies one of the above equivalent conditions.

Remark 3.1.9. When G is a finite constant group acting on a variety, if the action is faithful then it is automatically generically free. This fails in general for G a finite k-group scheme. For example the action $\alpha_p^2 \times_k \mathbb{A}^1_k \to \mathbb{A}^1_k$ given by $(a,b) \cdot x \mapsto x + ax^p + b$ is faithful (there is no non-trivial k-subgroup of α_p^2 acting trivially) but not generically free, in fact the stabilizer of the generic point η is $\mathrm{Stab}_G(\eta) = \mathrm{Spec}\,(k(x)[S,T]/(x^pS + T, S^p, T^p))$. Faithful actions coincide with generically free actions also for diagonalizable k-group schemes (this is known and we also give a proof in Corollary 3.3.2). Moreover, we show that this property holds, for instance, for infinitesimal commutative unipotent subgroup schemes of the k-group scheme of Witt vectors (see Remark 3.3.3).

Proposition 3.1.10. *Let G be a k-group scheme and X be a k-variety with a G-action. The G-action is generically free if and only if the induced $G_{\overline{k}}$-action on $X_{\overline{k}}$ is generically free.*

Proof. Let $\eta\colon \mathrm{Spec}(k(\eta)) \to X$ be the generic point of X. Since X is geometrically integral, then the generic point of $X_{\overline{k}}$ is the base change $\overline{\eta}\colon \mathrm{Spec}\left(k(\eta) \otimes_k \overline{k}\right) \to X_{\overline{k}}$ (see for example [Liu02, Chapter 3, Corollary 2.14]). Therefore, by general properties of the base change, we have that the stabilizer of $\overline{\eta}$ is

$$\mathrm{Stab}_{G_{\overline{k}}}(\overline{\eta}) \simeq \mathrm{Stab}_G(\eta)_{\overline{k}} \simeq \mathrm{Stab}_G(\eta) \times_{\mathrm{Spec}(k(\eta))} \mathrm{Spec}\left(k(\eta) \otimes_k \overline{k}\right)$$

where $\mathrm{Stab}_G(\eta)$ is the stabilizer of η. Now, since $k(\eta) \hookrightarrow k(\eta) \otimes_k \overline{k}$ is faithfully flat (it is a field extension since X is geometrically integral), then $\mathrm{Stab}_{G_{\overline{k}}}(\overline{\eta})$ is trivial (i.e. isomorphic to $\mathrm{Spec}\left(k(\eta) \otimes_k \overline{k}\right)$) if and only if $\mathrm{Stab}_G(\eta)$ is trivial (i.e. isomorphic to $\mathrm{Spec}(k(\eta))$), as wished. □

Before giving the definition of rational action, we recall what we mean by a rational (and birational) map between schemes.

Definition 3.1.11 (Rational map)**.** A *rational map* $f\colon Y \dashrightarrow Z$ of k-varieties is an equivalence class of pairs (U, φ), where U is a schematically dense open subset of Y, and $\varphi : U \to Z$ is a morphism; two pairs (U, φ) and (V, ψ) are equivalent if there exists a schematically dense open subset $W \subseteq U \cap V$ such that $\varphi_{|W} = \psi_{|W}$. Every rational map $f\colon Y \dashrightarrow Z$ has a unique representative (U, φ), where U is maximal; then U is the *domain of definition* $\mathrm{dom}(f)$ of f. The rational map f is *birational* if it admits a representative (U, φ) such that φ is an isomorphism onto a schematically dense open subset of Z.

Definition 3.1.12 (Rational action)**.** Let G be a finite k-group scheme and X a k-variety. A *rational action* of G on X is a rational map $\rho\colon G \times_k X \dashrightarrow X$ such that:

(i) the rational map $(\pi_1, \rho)\colon G \times_k X \dashrightarrow G \times_k X, (g, x) \dashmapsto (g, g \cdot x)$ is birational;

(ii) the following diagram commutes

$$\begin{array}{ccc} G \times_k G \times_k X & \xrightarrow{m \times \mathrm{id}_X} & G \times_k X \\ \downarrow{\scriptstyle \mathrm{id}_G \times \rho} & & \downarrow{\scriptstyle \rho} \\ G \times_k X & \xdashrightarrow{\rho} & X \end{array}$$

where $m\colon G \times_k G \to G$ denotes the multiplication morphism of G.

Let us stress that the two compositions of rational maps in the above diagram make sense. Indeed, as a consequence of (i), ρ is dominant, since it is the composition of the birational map (π_1, ρ) with the second projection. Therefore, the image of ρ contains a dense open subset $W \subseteq X$ and thus the image of $\mathrm{id}_G \times \rho$ contains $G \times_k W$. Let V denote the domain of definition of ρ; then the composite $\rho \circ (\mathrm{id}_G \times \rho)$ is defined on the open $(\mathrm{id}_G \times \rho)^{-1}(V \cap (G \times_k W))$. Moreover, the composite $\rho \circ (m \times \mathrm{id}_X)$ is defined since $m \times \mathrm{id}_X$ is a morphism.

Remark 3.1.13. Let X be a k-variety. There is a bijection between rational actions of G on X and G-actions on the generic point of X(see [Bri22, Corollary 3.4]).

Definition 3.1.14 (Faithful rational action)**.** Let G be a finite k-group scheme and X be a k-variety equipped with a rational action $\rho\colon G \times_k X \dashrightarrow X$. We say that it is a *faithful rational action* if the corresponding action on the generic point of X is faithful.

The following is a known result (see for example [TV13, Section 2]), we include the proof for the sake of completeness. The proof we give can be deduced from [Bri22, Lemma 5.3] where the case of curves is treated.

Proposition 3.1.15. *Let G be a finite k-group scheme and X be a k-variety endowed with a generically free rational G-action. Then*

$$\dim_k(\mathrm{Lie}(G)) \leq \dim(X).$$

Proof. Let U be an open subset of X on which the action is defined (see for example [Bri22, Proposition 3.2]). Suppose first that $char(k) = 0$, then G is étale, thus

$$0 = \dim_k(\mathrm{Lie}(G)) = \dim(G)$$

and the statement follows. Suppose then that $char(k) = p > 0$ and let G_1 be the kernel of the Frobenius morphism $F_G \colon G \to G^{(p)}$. Then G_1 is an infinitesimal k-subgroup scheme of G and $\mathrm{Lie}(G) = \mathrm{Lie}(G_1)$. If the G-action on U is generically free, then the same holds for G_1. We can thus suppose that $G = G_1$ and, by Proposition 3.1.10, that k is algebraically closed. By Proposition 3.1.7, the G-action is generically free if and only if X_{fr} is dense in X and thus there exists (since X is geometrically integral and $k = \overline{k}$) a smooth closed point $x \in U$ with trivial stabilizer $\mathrm{Stab}_G(x)$. Since G is infinitesimal, then also $\mathrm{Stab}_G(x)$ is such, hence $\mathrm{Stab}_G(x)$ is trivial if and only if $\mathrm{Lie}(\mathrm{Stab}_G(x))$ is trivial. Now, $\mathrm{Lie}(\mathrm{Stab}_G(x))$ is the kernel of the natural map $\mathrm{Lie}(G) \to T_xU$ (see [DG70, III.§2, 2.6]) and therefore if the action is generically free this map is an injection and thus the statement. □

Actions of finite group schemes and module algebras

Some references for this part are [DG70, II.§4, 5], [Swe69, Chapter VII] and [Mon93, Chapter 4]. Until the end of the section, $G = \mathrm{Spec}(A)$ will be a finite k-group scheme.

We begin by recalling the definition of differential operator, a central object when studying actions of infinitesimal group schemes. Let $X = \mathrm{Spec}(B)$ be an affine k-scheme. Every element $f \in B$ defines a map

$$\begin{aligned} \mathrm{ad}\,(f) : \mathrm{End}_k(B) &\to \mathrm{End}_k(B) \\ \varphi &\mapsto (g \mapsto f\varphi(g) - \varphi(fg)). \end{aligned}$$

Definition 3.1.16 (Differential operator)**.** A k-linear endomorphism φ of B is said to be a *differential operator* of order $\leq n$ if

$$\mathrm{ad}\,(f_0) \dots \mathrm{ad}\,(f_n)\varphi = 0$$

for all $f_0, \dots, f_n \in B$. Differential operators form a k-subalgebra $\mathrm{Diff}_k(B)$ of $\mathrm{End}_k(B)$.

Notice that differential operators of order ≤ 0 are B-linear endomorphisms and that differential operators φ of order ≤ 1 such that $\varphi(1) = 0$ are derivations on B.

Recall, from Definition 1.1.13 and Remark 1.1.14 in Chapter 1, that for A a k-Hopf algebra and B a k-algebra, B is said to be an *A-module algebra* if there exists

$$v \colon A \to \mathrm{End}_k(B), a \mapsto (b \mapsto a \cdot b)$$

which is a morphism of k-algebras satisfying the *property of compatibility with products*:

$$\begin{cases} v(a)(1) = \varepsilon(a) \\ v(a)(fg) = m_B(v \otimes v \circ \Delta(a))(f \otimes g) \end{cases}$$

for any $a \in A$ and $f, g \in B$, where ε denotes the counit of A, Δ its comultiplication and m_B the multiplication of B. Module algebras are very useful when studying actions of finite k-group schemes, thanks to the following result.

Proposition 3.1.17. *Let $G = \mathrm{Spec}(A)$ be a finite k-group scheme and $X = \mathrm{Spec}(B)$ be an affine k-scheme. There is a bijection between the set of right actions of G on X and the set of left $A^\vee$-module algebra structures on B.*

Proof. The bijection is obtained associating to any coaction $\rho\colon B \to B \otimes_k A$ the $A^\vee$-module algebra structure

$$\begin{aligned} v\colon A^\vee &\to \mathrm{End}_k(B) \\ \alpha &\mapsto (B \xrightarrow{\rho} B \otimes_k A \xrightarrow{\mathrm{id}_B \otimes \alpha} B \otimes_k k \simeq B). \end{aligned}$$

For more details see for example [Mon93, §4.1]. □

When dealing with infinitesimal group schemes, one can specialize Proposition 3.1.17 and prove that to give an action of these group schemes amounts to exhibiting a certain number of differential operators respecting some relations.

Proposition 3.1.18. *Let $G = \mathrm{Spec}(A)$ be an infinitesimal k-group scheme and $X = \mathrm{Spec}(B)$ be an affine k-scheme. There is a bijection between the set of right actions of G on X and the set of homomorphisms of k-algebras $v\colon A^\vee \to \mathrm{Diff}_k(B)$ such that*

$$v(\mu)(fg) = m_B(v \otimes v \circ \Delta(\mu))(f \otimes g) \tag{3.1}$$

for any $\mu \in A^\vee$ and $f, g \in B$, where Δ and m_B denote respectively the comultiplication of A and the multiplication of B.

Proof. See [DG70, II.§4, Proposition 7.2]. □

Example 3.1.19.

1. Consider the self-dual infinitesimal k-group scheme $\alpha_p = \mathrm{Spec}(k[T]/(T^p))$ whose group structure is given by

   $$\Delta(T) = T \otimes 1 + 1 \otimes T.$$

   To give an action of α_p on a k-scheme $X = \mathrm{Spec}(B)$ is equivalent to giving a k-linear derivation $\partial\colon B \to B$ such that $\partial^p = 0$.

2. Consider the purely transcendental extension $k(t)/k$. The algebra of differential operators $\mathrm{Diff}_k(k(t))$ is a $k(t)$-vector space with basis given by $\left\{\frac{\partial}{\partial t^i}\right\}$ where

   $$\frac{\partial}{\partial t^i}(t^r) = \begin{cases} \binom{r}{i} t^{r-i} & \text{if } r \geq i \\ 0 & \text{otherwise.} \end{cases}$$

   If k has characteristic zero, then $\frac{\partial}{\partial t^i} = \frac{1}{i!}\left(\frac{\partial}{\partial t}\right)^i$. On the other hand, if k has characteristic $p > 0$ this does not make sense for $i = 0 \mod p$. In this case if $i = jp^s$ for some $s \geq 0$ with $j \neq 0 \mod p$, then

   $$\frac{\partial}{\partial t^i} = \frac{\partial}{\partial t^{jp^s}} = \frac{1}{j!}\left(\frac{\partial}{\partial t^{p^s}}\right)^j.$$

   We will denote by ∂_{p^s} the differential operator $\frac{\partial}{\partial t^{p^s}}$.

3.2 Generically free rational actions

We begin this section with a useful criterion in order to determine when an action of an infinitesimal group scheme is generically free.

Proposition 3.2.1. *Let G be an infinitesimal k-group scheme and X an irreducible k-scheme endowed with a G-action. Then:*

1. *the G-action is generically free if and only if the induced $\ker(F_G)$-action is generically free;*
2. *if in addition k is perfect and G is commutative, the G-action is generically free if and only if the induced action of $\mathrm{soc}(G)$ is generically free.*

Proof.

1. Clearly if the G-action is generically free then also the induced $\ker(F_G)$-action is generically free. Suppose that the G-action on X is not generically free. Let η be the generic point of X and $K = k(\eta)$. Then $\mathrm{Stab}_G(\eta)$ is a non-trivial subgroup scheme of G_K and thus
$$\ker(F_{G_K}) \times_{G_K} \mathrm{Stab}_G(\eta) = \ker(F_G)_K \times_{G_K} \mathrm{Stab}_G(\eta) \overset{3.1.6}{=} \mathrm{Stab}_{\ker(F_G)}(\eta)$$
is non-trivial. Therefore the action of $\ker(F_G)$ on X is not generically free.
2. Clearly if the G-action is generically free then also the induced $\mathrm{soc}(G)$-action is generically free. For the other way around, by Proposition 3.1.10 and Lemma 2.2.26 we may suppose that $k = \overline{k}$. Then G is trigonalizable. Suppose by contradiction that the G-action on X is not generically free. Let η be the generic point of X and $K = k(\eta)$. Then $\mathrm{Stab}_G(\eta)$ is a non-trivial subgroup scheme of G_K and thus
$$\mathrm{soc}(\mathrm{Stab}_G(\eta)) \overset{2.2.19}{=} \mathrm{soc}(G_K) \times_{G_K} \mathrm{Stab}_G(\eta) \overset{2.2.26}{=}$$
$$\mathrm{soc}(G)_K \times_{G_K} \mathrm{Stab}_G(\eta) \overset{3.1.6}{=} \mathrm{Stab}_{\mathrm{soc}(G)}(\eta)$$
is non-trivial by Lemma 2.2.19. Therefore the action of $\mathrm{soc}(G)$ on X is not generically free which gives a contradiction.

□

Recall the following definition.

Definition 3.2.2 (Solvable group scheme)**.** A k-group scheme G is said to be *k-solvable* if it is affine and it admits a composition series with quotients isomorphic either to $\mathbb{G}_{a,k}$ or to $\mathbb{G}_{m,k}$ (see for example [DG70, IV.§4, Definition 3.1]).

Proposition 3.2.3. *Let G be a k-group scheme.*

1. *If G is k-solvable, then G is trigonalizable and its maximal unipotent k-subgroup scheme G^u is k-solvable. Moreover G is isomorphic as a k-scheme to $\mathbb{G}_{m,k}^{n-r} \times_k \mathbb{G}_{a,k}^r$ where $n = \dim(G)$ and $r = \dim(G^u)$.*

2. *If k is perfect and G is trigonalizable, smooth and connected, then G is k-solvable.*

Proof. See for example [DG70, IV.§4, Proposition 3.4 and Corollary 3.8]. □

The following Proposition proves the existence part of Theorem 3.2.13 in the case of commutative trigonalizable group schemes of height one (see Remark 3.2.5).

Proposition 3.2.4. *Let $\mathcal{G}$ be a k-solvable group scheme of dimension n, consider $G = \ker(F_{\mathcal{G}}^s \colon \mathcal{G} \to \mathcal{G})$ for some $s \geq 1$ and let X be a k-variety of dimension ℓ. Then there exist generically free rational actions of G on X if and only if $n \leq \ell$.*

Proof. Suppose that there exists a generically free rational action of G on X. Then, by Proposition 3.1.15,

$$n = \dim(\mathcal{G}) = \dim_k(\mathrm{Lie}(G)) \leq \dim(X) = \ell.$$

For the converse, let us start by proving that any variety X of dimension ℓ admits a generically free rational action of G if $n = \ell$. By Proposition 3.2.3, G is a subscheme of

$$\mathcal{G} \simeq \mathbb{G}_{m,k}^{n-r} \times_k \mathbb{G}_{a,k}^r$$

where $r = \dim(\mathcal{G}^u)$ and thus there is a natural generically free G-action on $\mathbb{G}_{m,k}^{n-r} \times_k \mathbb{G}_{a,k}^r$ by multiplication, since G is a subgroup scheme of $\mathcal{G}$. We then have the G-torsor given by the Frobenius

$$F^s \colon \mathbb{G}_{m,k}^{n-r} \times_k \mathbb{G}_{a,k}^r \to \mathbb{G}_{m,k}^{n-r} \times_k \mathbb{G}_{a,k}^r.$$

Let $K = k(X)$ and take any point $x \in \left(\mathbb{G}_{m,k}^{n-r} \times_k \mathbb{G}_{a,k}^r\right)\left(kK^{p^s}\right)$,

$$x = (x_1, \ldots, x_n) \colon \mathrm{Spec}\left(kK^{p^s}\right) \to \mathbb{G}_{m,k}^{n-r} \times_k \mathbb{G}_{a,k}^r.$$

Then we have a G-torsor

$$Y_x = \mathrm{Spec}\left(kK^{p^s}[T_1, \ldots, T_n]/(T_i^{p^s} - x_i)_{i=1,\ldots,n}\right) \longrightarrow \mathrm{Spec}(kK^{p^s})$$

given by the pull-back diagram

$$\begin{array}{ccc} Y_x & \longrightarrow & \mathrm{Spec}(kK^{p^s}) \\ \downarrow & & \downarrow x \\ \mathbb{G}_{m,k}^{n-r} \times_k \mathbb{G}_{a,k}^r & \xrightarrow{F^s} & \mathbb{G}_{m,k}^{n-r} \times_k \mathbb{G}_{a,k}^r. \end{array}$$

Let $\{y_1, \dots, y_n\}$ be a p-basis for K/kK^p and $x = (x_1, \dots, x_n) \in \left(\mathbb{G}_{m,k}^{n-r} \times_k \mathbb{G}_{a,k}^r\right)\left(kK^{p^s}\right)$ be the point with coordinates $x_i = y_i^{p^s}$ for $i = 1, \dots, n$. Let us show that there is an isomorphism

$$kK^{p^s}[T_1, \dots, T_n]/(T_i^{p^s} - x_i)_{i=1,\dots,n} \simeq K, T_i \mapsto y_i.$$

First of all, let us see that $kK^{p^s}[T_1, \dots, T_n]/(T_i^{p^s} - x_i)_{i=1,\dots,n}$ is a field. We can see this by induction on n: in fact,

$$kK^{p^s}[T_1]/(T_1^{p^s} - x_1)$$

is a field since $T_1^{p^s} - x_1$ is irreducible in $kK^{p^s}[T_1]$ since $y_1 \notin kK^p$. Without loss of generality we can then suppose by induction that

$$L := kK^{p^s}[T_1, \dots, T_{n-1}]/(T_i^{p^s} - x_i)_{i=1,\dots,n-1}$$

is a field and consider

$$L[T_n]/(T_n^{p^s} - x_n).$$

The polynomial $T_n^{p^s} - x_n$ is irreducible in $L[T_n]$ since $y_n \notin kK^p$ and thus the claim. Consider the morphism of rings

$$\begin{aligned} \psi \colon kK^{p^s}[T_1, \dots, T_n]/(T_i^{p^s} - x_i)_{i=1,\dots,n} &\to K \\ T_i &\mapsto y_i, \end{aligned}$$

then, since the objects are fields, it is an injection and since the two fields have the same degree over kK^{p^s} then ψ is an isomorphism, as wished. Therefore we constructed a G-torsor $Y_x = \operatorname{Spec}(K) \to \operatorname{Spec}(kK^{p^s})$, that is there exists a generically free rational action of G on X, as claimed. For the general case, consider

$$H = \ker(F^s \colon \mathcal{G} \times_k \mathbb{G}_a^{\ell-n} \to \mathcal{G} \times_k \mathbb{G}_a^{\ell-n}).$$

By what we have just proved, there exists a generically free rational action of H on X, since

$$\dim(\mathcal{G} \times_k \mathbb{G}_a^{\ell-n}) = \ell = \dim(X).$$

Notice that $G = \ker(F^s \colon \mathcal{G} \to \mathcal{G})$ is a k-subgroup scheme of H, indeed it is the kernel of the projection

$$\pi_2 \colon H \to \mathbb{G}_a^{\ell-n}.$$

As a consequence, there exists also a generically free rational action of G on X, as wished. □

Remark 3.2.5. If k is perfect and G is a commutative trigonalizable k-group scheme of height one, then

$$G \simeq \prod_{i=1}^{t} W_{n_i}^1 \times_k \mu_p^l = \ker\left(F \colon \prod_{i=1}^{t} W_{n_i} \times_k \mathbb{G}_m^l \to \prod_{i=1}^{t} W_{n_i} \times_k \mathbb{G}_m^l\right)$$

for some $t, l, n_i \geq 1$ (see for example [DG70, IV.§2, 2.14]) and $\prod_{i=1}^{t} W_{n_i} \times_k \mathbb{G}_m^l$ is a k-solvable group scheme of dimension equal to $\dim_k(\operatorname{Lie}(G))$. Hence, Proposition 3.2.4 applies in this case with $n = \dim_k(\operatorname{Lie}(G))$.

The following is an asymptotic result for the dimension of varieties endowed with generically free rational actions of infinitesimal unipotent group schemes. This result will be made more precise in the commutative case and over a perfect field with Theorem 3.2.13.

Corollary 3.2.6. *For every infinitesimal trigonalizable k-group scheme G there exists an integer $r > 0$ such that for every variety X of dimension $\geq r$ there exist generically free rational actions of G on X.*

Proof. Any trigonalizable k-group scheme G has a closed immersion in the smooth k-algebraic group T_n of upper triangular matrices for some n. This k-group scheme is k-solvable. Moreover, if G is infinitesimal, it is contained in the kernel of some power of the Frobenius of T_n. Therefore, by the previous Proposition, any variety of dimension greater than or equal to the dimension of T_n admits a generically free G-action. □

Remark 3.2.7. Notice that, as a consequence of the above Proposition 3.2.4, we have that for every variety X of dimension n and for any $j \leq n$, there exists a nilpotent k-linear derivation D on $K = k(X)$ of order p^j. Indeed, consider a generically free rational action of W_j^1 on X which corresponds to a module algebra structure

$$\begin{aligned} k[T]/(T^{p^j}) &\to \mathrm{Der}_k(K) \\ T &\mapsto D \end{aligned}$$

where $k[T]/(T^{p^j})$ represents α_{p^j}, the Cartier dual of W_j^1. Then $D^{p^j} = 0$ and, by [DG70, III.§2, Corollary 2.7], $D, D^p, \ldots, D^{p^{j-1}}$ are K-linearly independent, hence D has order j.

Proof of Theorem 3.2.13

We begin this part with three technical results that are the building blocks for the construction of generically free rational actions done in the proof of Theorem 3.2.13: the main idea of the proof is to show that for G an infinitesimal commutative unipotent k-group scheme of height n, a generically free rational action of $G_{n-1} = \ker(F_G^{n-1})$ on a variety X can be extended to a rational action of G. Lemma 3.2.8 tells us that if G_{n-1} acts on X, then G acts already on $X^{(p)}$. Lemma 3.2.10 shows that to extend a rational action of G_{n-1}, it is enough to define it on a p-basis of the fraction field $K = k(X)/kK^p$. Lemma 3.2.11 shows that under certain commutativity assumptions, some commutators are indeed derivations on K.

Lemma 3.2.8. *Let G be an infinitesimal k-group scheme of height n and let us denote $G_i := \ker(F_G^i)$ for all $i = 1, \ldots, n-1$. Any action of G_{n-1} on a k-variety X induces naturally an action of G/G_i on $X^{(p^i)}$ for $i = 1, \ldots, n-1$. Moreover, if the G_{n-1}-action on X is faithful, the same holds true for the induced G/G_i-action on $X^{(p^i)}$.*

Proof. Let $G_{n-1} \times_k X \to X$ be a faithful action. Then we have a naturally induced faithful action $G_{n-1}^{(p^i)} \times_k X^{(p^i)} \to X^{(p^i)}$ obtained by base change (the proof is the same as

that of Lemma 3.1.4) and therefore also of

$$G/G_i \simeq \mathrm{Im}(F_G^i) \subseteq G_{n-1}^{(p^i)}$$

on $X^{(p^i)}$. □

Remark 3.2.9.

- In the above setting, the composite

  $$G \times_k X^{(p)} \to G/\ker(F_G) \times_k X^{(p)} \to X^{(p)}$$

  provides us naturally with an action of G on $X^{(p)}$, via $F_G\colon G \to G^{(p)}$.

- Algebraically, this means that if we have a module algebra structure

  $$k[G_{n-1}^\vee] \to \mathrm{End}_k(B)$$

  this induces a module algebra structure

  $$v\colon k[G^\vee] \to \mathrm{End}_k(\mathrm{Im}(F_B)).$$

  Let $\eta\colon \mathrm{Im}(F_B) \to \mathrm{Hom}_k\left(k[G^\vee], \mathrm{Im}(F_B)\right)$ be the corresponding morphism of algebras. Explicitly we then have that for every $a \in k[G^\vee]$ and $\beta \in B^{(p)}$ it holds

  $$\eta(F_B(\beta))(a) = \left(F_{\mathrm{Hom}_k(A,B)} \circ \eta^{(p)}(\beta)\right)(a) =$$

  $$F_B \circ \eta^{(p)}(\beta) \circ V_A(a) = F_B(v^{(p)}(V_A(a))(\beta))$$

  where the first equality holds by functoriality of the Frobenius and the second one by Lemma 2.2.3.

Let k be perfect, G be an infinitesimal commutative unipotent k-group scheme of height n and $G_{n-1} = \ker(F_G^{n-1})$. In order to simplify the notation we denote by $G_{n-1}^\vee$ its dual, that is $G_{n-1}^\vee := (G_{n-1})^\vee = \mathrm{coker}(V_{G^\vee}^{n-1}) = G^\vee/\mathrm{Im}(V_{G^\vee}^{n-1})$. In Proposition 2.2.30, we showed that there exists a structure of k-group scheme on $\mathcal{G} := G_{n-1}^\vee \times_k \mathbb{A}_k^{r_n}$ where $r_n = \dim_k(\mathrm{Lie}(\mathrm{Im}(V_{G^\vee}^{n-1})))$ such that

$$0 \to \mathbb{G}_a^{r_n} \to \mathcal{G} \to G_{n-1}^\vee \to 0.$$

Moreover, $G^\vee$ embeds in $\mathcal{G}$ realizing the exact sequence

$$0 \to G^\vee \to \mathcal{G} \to \mathbb{G}_a^{r_n} \to 0.$$

At the level of algebras, this is rephrased by saying that

$$k[\mathcal{G}] = k[G_{n-1}^\vee][T_1, \ldots, T_{r_n}]$$

can be endowed with a structure of k-Hopf algebra (coming from that of Witt vectors) such that

$$\Delta(T_j) = T_j \otimes 1 + 1 \otimes T_j + R_j$$

where R_j is an element of $k[G_{n-1}^\vee] \otimes_k k[G_{n-1}^\vee]$. Moreover,

$$k[G^\vee] = k[G_{n-1}^\vee][T_1, \dots, T_{r_n}]/(P_1, \dots, P_{r_n})$$

where the polynomials P_j are primitive elements of $k[G_{n-1}^\vee][T_1, \dots, T_{r_n}]$ congruent to $T_j^{p^{l_j}}$ for some $l_j \geq 1$ modulo the augmentation ideal of $k[G_{n-1}^\vee]$ for every $j = 1, \dots, r_n$.

For any $r \leq \dim_k(\mathrm{Lie}(\mathrm{Im}(V_{G^\vee}^{n-1})))$, consider the commutative k-Hopf algebra

$$k[G_{n-1}^\vee][T_1, \dots, T_r]$$

corresponding to $G_{n-1}^\vee \times_k \mathbb{A}_k^r$ with k-group scheme structure induced by that of $\mathcal{G}$. Consider the non-commutative k-algebra $k[G_{n-1}^\vee]\langle T_1, \dots, T_r\rangle$ where the variables T_i don't commute neither among them nor with the commutative subalgebra $k[G_{n-1}^\vee]$. We endow $k[G_{n-1}^\vee]\langle T_1, \dots, T_r\rangle$ of a k-Hopf algebra structure (which extends that of $k[G_{n-1}^\vee]$) defined as follows: one first takes the non-commutative free algebra $\Gamma = k\langle T_{ij}, T_1, \dots, T_r\rangle_{1\leq i\leq n-1, 1\leq j\leq s}$ where s is minimal such that $G_{n-1}^\vee \subseteq (W_{n-1})^s$ (notice that the T_{ij}'s are the variables needed to define $k[G_{n-1}^\vee]$, while the r additional variables $T_1, \dots, T_r$ will each play the role of the nth coordinate in the corresponding copy of Witt vectors). We define $\Delta : \Gamma \to \Gamma \otimes_k \Gamma$, sending each variable to the element of $\Gamma \otimes_k \Gamma$ given by the comultiplication of commutative Witt vectors and then extending this map to a morphism of algebras. Finally we quotient Γ by the two-sided ideal given by the commutators of the variables T_{ij} for $1 \leq i \leq n-1, 1 \leq j \leq s$ and by the two-sided ideal defining $k[G_{n-1}^\vee]$. In this way, Δ defines a comultiplication on $k[G_{n-1}^\vee]\langle T_1, \dots, T_r\rangle$ (before taking the quotient Δ was not a priori coassociative). In this setting, we have the following results.

Lemma 3.2.10. *Let X be a k-variety of dimension s with fraction field K and p-basis $(t_1, \dots, t_s)$ of K/kK^p. Then for any set $\{x_{ih} \mid i = 1, \dots, r, h = 1, \dots, s\}$ of elements of K and any module algebra structure*

$$\tilde{v} \colon k[G_{n-1}^\vee] \to \mathrm{Diff}_k(K)$$

there exists a unique module algebra structure

$$v \colon k[G_{n-1}^\vee]\langle T_1, \dots, T_r\rangle \to \mathrm{Diff}_k(K)$$

extending $\tilde{v}$ and such that $v(T_i)(t_h) = x_{ih}$ for every i and h.

Proof. Let us begin with the existence. Since $v_{|k[G_{n-1}^\vee]} = \tilde{v}$, it is enough to show that we can define $D_i = v(T_i)$ satisfying the property of compatibility with products (1.1) and such that $D_i(t_h) = x_{ih}$ for every i and h. By Proposition 2.2.30 we have

$$\Delta(T_i) = T_i \otimes 1 + 1 \otimes T_i + \sum_j \alpha_{ij} \otimes \beta_{ij}$$

with α_{ij} and β_{ij} lying in $k[G_{n-1}^\vee]$ for all i, j. Therefore we need to define D_i in such a way that

$$D_i(fg) = D_i(f)g + fD_i(g) + \sum_j v(\alpha_{ij})(f)v(\beta_{ij})(g)$$

for all $f, g \in K$. Recall that for $(t_1, \dots, t_s)$ to be a p-basis of K/kK^p means that

$$\{t_1^{m_1} \dots t_s^{m_s} \mid 0 \leq m_1, \dots, m_s \leq p-1\}$$

is a basis of K as kK^p-vector space. By assumption G_{n-1} acts on the generic point $Y = \mathrm{Spec}(K)$ of X and thus, by Lemma 3.2.8, G acts on $Y^{(p)} = \mathrm{Spec}(kK^p)$. Therefore, the differential operator $D_i := v(T_i)$ is defined on kK^p for every $i = 1, \dots, r$. We then define

$$D_i(at_h) = D_i(a)t_h + ax_{ih} + \sum_j v(\alpha_{ij})(a)v(\beta_{ij})(t_h)$$

and

$$D_i(t_h t_l) = x_{ih}t_l + t_h x_{il} + \sum_j v(\alpha_{ij})(t_h)v(\beta_{ij})(t_l)$$

for every $a \in kK^p$ and $h \leq l = 1, \dots, s$. Applying recursively the formula

$$D_i(fg) = D_i(f)g + fD_i(g) + \sum_j v(\alpha_{ij})(f)v(\beta_{ij})(g)$$

we define D_i on all the monomials of the form $at_1^{m_1} \dots t_s^{m_s}$ with $a \in kK^p$ and $0 \leq m_1, \dots, m_s \leq p-1$ and extend it by linearity to every element of K. The fact that D_i is well-defined is a consequence of the coassociativity and cocommutativity of the Hopf algebra structure on $k[G_{n-1}^\vee]\langle T_1, \dots, T_r\rangle$. The uniqueness of the module algebra structure comes by construction. □

Given two strings of natural numbers $I = (i_1, \dots, i_n)$ and $J = (j_1, \dots, j_n)$, we say that I is smaller than J with respect to the lexicographic order, and we write $I <_{LEX} J$, if there exists $k \in \{1, \dots, n\}$ such that $(i_1, \dots, i_{k-1}) = (j_1, \dots, j_{k-1})$ and $i_k < j_k$.

Lemma 3.2.11. *Let $A := k[G_{n-1}^\vee]\langle T_{n1}, \dots, T_{nr_n}\rangle$ be as above. Moreover, write*

$$k[G_j^\vee] = k[G_{j-1}^\vee][T_{j1}, \dots, T_{jr_j}]/(P_{j1}, \dots, P_{jr_j})$$

as in Remark 2.2.31 for every $j \leq n-1$. Let

$$v \colon A \to \mathrm{End}_k(B)$$

be an A-module algebra structure on a k-algebra B and let $D_{jh} := v(T_{jh})$ for every $j = 1, \dots, n$ and $h = 1, \dots, r_j$. It holds that for any $h = 1, \dots, r_n$ and $(s,t) <_{LEX} (n,h)$, if D_{nh} commutes with every element of $v\left(k[G_{s-1}]\right)$ then $D_{nh}D_{st} - D_{st}D_{nh}$ is a derivation.

Proof. Recall that, by Proposition 2.2.30, for every $j = 1, \dots, n$ and $h = 1, \dots, r_j$

$$\Delta(T_{jh}) = T_{jh} \otimes 1 + 1 \otimes T_{jh} + \sum_q \alpha_{jh}^q \otimes \beta_{jh}^q$$

where α_{jh}^q and β_{jh}^q lie in $k[G_{j-1}^\vee]$ for all q. Now

$$\Delta(T_{nh}T_{st}) = \Delta(T_{nh})\Delta(T_{st}) =$$

$$T_{nh}T_{st} \otimes 1 + 1 \otimes T_{nh}T_{st} + T_{nh} \otimes T_{st} + T_{st} \otimes T_{nh} +$$

$$\sum_q \alpha_{nh}^q T_{st} \otimes \beta_{nh}^q + \sum_q \alpha_{nh}^q \otimes \beta_{nh}^q T_{st} + \sum_{q'} T_{nh}\alpha_{st}^{q'} \otimes \beta_{st}^{q'} + \sum_{q'} \alpha_{st}^{q'} \otimes T_{nh}\beta_{st}^{q'} + \sum_{q,q'} \alpha_{nh}^q \alpha_{st}^{q'} \otimes \beta_{nh}^q \beta_{st}^{q'}$$

and

$$\Delta(T_{st}T_{nh}) = \Delta(T_{st})\Delta(T_{nh}) =$$

$$T_{st}T_{nh} \otimes 1 + 1 \otimes T_{st}T_{nh} + T_{nh} \otimes T_{st} + T_{st} \otimes T_{nh} +$$

$$\sum_q T_{st}\alpha_{nh}^q \otimes \beta_{nh}^q + \sum_q \alpha_{nh}^q \otimes T_{st}\beta_{nh}^q + \sum_{q'} \alpha_{st}^{q'} T_{nh} \otimes \beta_{st}^{q'} + \sum_{q'} \alpha_{st}^{q'} \otimes \beta_{st}^{q'} T_{nh} + \sum_{q,q'} \alpha_{st}^{q'} \alpha_{nh}^q \otimes \beta_{st}^{q'} \beta_{nh}^q.$$

Therefore

$$\Delta(T_{nh}T_{st} - T_{st}T_{nh}) =$$

$$(T_{nh}T_{st} - T_{st}T_{nh}) \otimes 1 + 1 \otimes (T_{nh}T_{st} - T_{st}T_{nh}) +$$

$$\sum_q \alpha_{nh}^q T_{st} \otimes \beta_{nh}^q + \sum_q \alpha_{nh}^q \otimes \beta_{nh}^q T_{st} + \sum_{q'} T_{nh}\alpha_{st}^{q'} \otimes \beta_{st}^{q'} + \sum_{q'} \alpha_{st}^{q'} \otimes T_{nh}\beta_{st}^{q'}$$

$$- \sum_q T_{st}\alpha_{nh}^q \otimes \beta_{nh}^q - \sum_q \alpha_{nh}^q \otimes T_{st}\beta_{nh}^q - \sum_{q'} \alpha_{st}^{q'} T_{nh} \otimes \beta_{st}^{q'} - \sum_{q'} \alpha_{st}^{q'} \otimes \beta_{st}^{q'} T_{nh}.$$

If $(s,t) <_{LEX} (n,h)$, using the hypothesis that D_{nh} commutes with every element of $v\,(k[G_{s-1}])$ we obtain that

$$(D_{nh}D_{st} - D_{st}D_{nh})(fg) = m \circ (v \otimes v \circ \Delta(T_{nh}T_{st} - T_{st}T_{nh}))(f \otimes g) =$$

$$m \circ (v \otimes v \circ (T_{nh}T_{st} - T_{st}T_{nh}) \otimes 1 + 1 \otimes (T_{nh}T_{st} - T_{st}T_{nh}))(f \otimes g)$$

for every $f, g \in B$. Hence the statement. □

We give now an example, showing how to construct explicitly generically free rational actions of the p^m-torsion of a supersingular elliptic curve on any curve. The aim is that the understanding of this baby case will help in getting through the proof of Theorem 3.2.13.

Example 3.2.12. Take the self-dual infinitesimal commutative unipotent k-group scheme

$$G = \ker(F - V \colon W_n^n \to W_n^n) = \operatorname{Spec}\left(k[T_1, \ldots, T_n]/(T_1^p, T_2^p - T_1, \ldots, T_n^p - T_{n-1})\right).$$

If k is algebraically closed, and $n = 2m$, G is the p^m-torsion of any supersingular elliptic curve over k (see Corollary 2.3.10). Let X be any curve over k and $K = kK^p(t)$ be its function field, with p-basis $\{t\}$ over kK^p. Since G is self-dual, to give a rational G-action on X is equivalent to giving a module algebra structure

$$v \colon \operatorname{Spec}\left(k[U_1, \ldots, U_n]/(U_1^p, U_2^p - U_1, \ldots, U_n^p - U_{n-1})\right) \to \operatorname{Diff}_k(K).$$

We know that there exist generically free rational actions of the Frobenius kernel

$$\ker(F_G) = \operatorname{Spec}(k[T_n]/(T_n^p)) \simeq \alpha_p$$

on X. In particular, any such action corresponds to choosing a non-zero derivation D_1 on K of order p (see Definition 1.2.2) or, equivalently, to giving a module algebra structure

$$v \colon \operatorname{Spec}\left(k[U_1]/(U_1^p)\right) \to \operatorname{Diff}_k(K).$$

We want to show that any such action can be extended to a generically free rational action of G on X. To do so we show that for any $i = 2, \ldots, n$ any generically free rational action of $\ker(F_G^{i-1})$ on X extends to a generically free rational action of $\ker(F_G^i)$. Notice that

$$\ker(F_G^i) = \operatorname{Spec}\left(k[T_{n-i+1}, \ldots, T_n]/(T_{n-i+1}^p, T_{n-i+2}^p - T_{n-i+1}, \ldots, T_n^p - T_{n-1})\right)$$

and that to give a rational action of $\ker(F_G^i)$ on X is equivalent to defining a module algebra structure

$$v \colon \operatorname{Spec}\left(k[U_1, \ldots, U_i]/(U_1^p, U_2^p - U_1, \ldots, U_i^p - U_{i-1})\right) \to \operatorname{Diff}_k(K).$$

Suppose then that we have a generically free rational action of $\ker(F_G^{i-1})$ given by differential operators $D_1, \ldots, D_{i-1}$ where $D_j = v(T_j)$ for every $j = 1, \ldots, i-1$. To extend it to a rational action of $\ker(F_G^i)$ is equivalent to defining a differential operator $D_i = v(T_i)$ such that:

1. D_i respects the property of compatibility with products (1.1);
2. D_i commutes with D_j for every $j = 1, \ldots, i-1$;
3. $D_i^p = D_{i-1}$.

By Lemma 3.2.8, D_i is defined on kK^p. In particular,

$$D_i(\beta^p) = v(T_i)(\beta^p) = (v(V(T_i))(\beta))^p = (D_{i-1}(\beta))^p$$

for every $\beta \in K$. By Lemma 3.2.10, we then have that D_i is defined using property 1, provided we choose $x = D_i(t)$. Therefore, the first property is respected by definition

and we need to show that there exists x such that also properties 2 and 3 are satisfied. By Lemma 3.2.11 and the fact that $T_i^p - T_{i-1}$ is a primitive element, we have that $D_iD_j - D_jD_i$ and $D_i^p - D_{i-1}$ are derivations for every $j = 1, \dots, i-1$. Applying Remark 1.2.5, we obtain that D_i commutes with D_j for every $j = 1, \dots, i-1$ and $D_i^p = D_{i-1}$ if and only if the system

$$\begin{cases} D_j(x) = D_iD_j(t) & j = 1, \dots, i-1 \\ D_i^{p-1}(x) = D_{i-1}(t) \end{cases}$$

admits a solution $x = D(t)$. Notice first of all that the system is well-defined, that is D_i is defined on $D_j(t)$. In fact, by Corollary 1.2.3 we can suppose that $D_1(t) = 1$, therefore $D_1D_j(t) = D_jD_1(t) = D_j(1) = 0$, that is $D_j(t)$ belongs to kK^p, on which D_i is defined. Let $a_j := D_iD_j(t)$ for $j = 1, \dots, i-1$. By induction, the set $\{D_1, \dots, D_{i-1}\}$ is an ordered set of pairwise commuting differential operators and such that D_j is a derivation of order p on the subfield $K^{D_1,\dots,D_{j-1}}$. Moreover,

$$D_j(a_l) = D_l(a_j)$$

for all $j, l = 1, \dots, i-1$, indeed by induction

$$D_jD_l(t) = D_lD_j(t)$$

and thus

$$D_j(a_l) = D_jD_iD_l(t) = D_iD_jD_l(t) = D_iD_lD_j(t) = D_lD_iD_j(t) = D_l(a_j)$$

as wished (we used the fact that D_i satisfies properties 2 and 3 on kK^p). Moreover, $D_j^p = D_{j-1}$. By Corollary 1.2.7 we then know that a solution of the system

$$S = \begin{cases} D_1(x) = a_1 \\ \vdots \\ D_{i-1}(x) = a_{i-1} \end{cases}$$

exists if and only if

$$D_j^{p-1}(a_j) = a_{j-1}$$

for all $j = 1, \dots, i-1$. The relation indeed holds true, in fact

$$D_j^{p-1}(a_j) = D_j^{p-1}D_iD_j(t) = D_iD_j^p(t) = D_iD_{j-1}(t) = a_{j-1}$$

where again we used the fact that $D_j(t) \in kK^p$ and that D_i commutes with the other differential operators on kK^p. We are left to find a solution of S which satisfies also the last equation

$$D_i^{p-1}(x) = D_{i-1}(t).$$

Let then z be a solution of S: we are looking for another solution of S of the form $x = z + y$ with $y \in K^{D_1,\dots,D_{i-1}}$. Therefore x is solution of

$$D_i^{p-1}(x) = D_{i-1}(t)$$

if and only if

$$D_i^{p-1}(y) = D_{i-1}(t) - D_i^{p-1}(z).$$

Notice that the right hand side belongs to $K^{D_1,\dots,D_{i-1}} \subseteq kK^p$ on which D_i is a derivation of order p. Indeed, for every $j = 1, \dots, i-1$ it holds

$$D_j D_i^{p-1}(z) = D_i^{p-1} D_j(z) = D_i^{p-1} D_i D_j(t) = D_i^p D_j(t) = D_{i-1} D_j(t) = D_j D_{i-1}(t)$$

as wished. Therefore, by Lemma 1.2.3, y exists if and only if $D_i(D_{i-1}(t) - D_i^{p-1}(z)) = 0$ which is satisfied since

$$D_i^p(z) = D_{i-1}(z) = D_i D_{i-1}(t).$$

Notice that the action constructed is generically free since it extends the generically free action of $\mathrm{soc}(G)$ (see Proposition 3.2.1).

We are now ready to prove our result in full generality.

Theorem 3.2.13. *Let k be a perfect field of characteristic $p > 0$ and G be an infinitesimal commutative unipotent k-group scheme with Lie algebra of dimension s. Then for every k-variety X of dimension $\geq s$ there exist generically free rational actions of G on X. Moreover, for any $r \geq 1$, any generically free rational action of $\ker(F_G^r)$ on X can be extended to a generically free rational action of G on X.*

Proof. We begin by proving that if X is a k-variety of dimension $s = \dim_k(\mathrm{Lie}(G))$, then X admits a generically free rational action of G. By Proposition 3.2.4 and Remark 3.2.5, there exists a generically free rational action of $\ker(F_G)$ on X. Consider the filtration

$$G_1 \subseteq G_2 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$$

where $G_i := \ker(F_G^i)$ and n is the height of G.

First recurrence (on i):

To show that there exists a generically free rational action of G on X, we will prove that for every $i = 2, \dots, n$ any generically free rational action of G_{i-1} on X extends to a generically free rational action of G_i on X. Moreover, we will consider any possible extension of the actions. As a consequence, the second part of the statement will be satisfied by construction. Let $K = k(X)$ be the function field of X. By Proposition 3.1.18, to give a rational action of G_i on X is equivalent to endowing K with a $k[G_i^\vee]$-module algebra structure, where $G_i^\vee$ is the Cartier dual of G_i. By Proposition 2.2.30,

$$k[G_i^\vee] = k[G_{i-1}^\vee][T_{i1}, \dots, T_{ir_i}]/(P_{i1}, \dots, P_{ir_i})$$

where

$$G_{i-1}^\vee = \mathrm{coker}(V_{G^\vee}^{i-1}) = \left(\ker(F_G^{i-1})\right)^\vee,$$

$r_i = \dim_k(\mathrm{Lie}(H_i))$ with $H_i = \mathrm{Im}(V_{G^\vee}^{i-1})/\mathrm{Im}(V_{G^\vee}^{i})$, $P_{ij} = T_{ij}^{p^{m_{ij}}} - Q_{ij}$ are primitive elements of $k[G_{i-1}^\vee][T_{i1}, \dots, T_{ir_i}]$, Q_{ij} are polynomials with coefficients in the augmentation ideal of $k[G_{i-1}^\vee]$ and

$$\Delta(T_{ij}) = T_{ij} \otimes 1 + 1 \otimes T_{ij} + R_{ij}$$

where R_{ij} is an element of $k[G_{i-1}^\vee] \otimes_k k[G_{i-1}^\vee]$ for every $j = 1, \dots, r_i$. We then want to show that a $k[G_{i-1}^\vee]$-module algebra structure on K extends to a $k[G_i^\vee]$-module algebra structure on K. A $k[G_{i-1}^\vee]$-module structure on K is given by a morphism of algebras

$$v\colon k[G_{i-1}^\vee] \to \mathrm{Diff}_k(K)$$

respecting the property of compatibility with products (see Proposition 3.1.18). If we want to extend v to

$$k[G_i^\vee] = k[G_{i-1}^\vee][T_{i1}, \dots, T_{ir_i}]/(T_{i1}^{p^{m_{i1}}} - Q_{i1}, \dots, T_{ir_i}^{p^{m_{ir_i}}} - Q_{ir_i}) \to \mathrm{Diff}_k(k(X))$$

we need to define $v(T_{ij}) = D_{ij}$ for every $j = 1, \dots, r_i$ in such a way that the above map is a $k[G_i^\vee]$-module algebra structure on K, that is the following properties are satisfied for every $j = 1, \dots, r_i$:

1. D_{ij} respects the property of compatibility with products;
2. D_{ij} commutes with D_{kl} for every $(k, l) <_{LEX} (i, j)$;
3. $D_{ij}^{p^{m_{ij}}} = v(Q_{ij})$.

Notice that

$$\ker(F_G) \simeq \prod_{j \in I} W_{m_{1j}}^1$$

where I is a finite set and $\sum_{j \in I} m_{1j} = s$ which is the dimension of $\mathrm{Lie}(G)$. Then

$$(\ker(F_G))^\vee \simeq \prod_{j \in I} \alpha_{p^{m_{1j}}}$$

and thus, by [DG70, III.§2, Corollary 2.7], to give a generically free rational action of $\ker(F_G)$ on X corresponds to giving a set of derivations $\{D_{1j}\}_{j \in I}$ on K commuting pairwise and with D_{1j} of order $p^{m_{1j}}$ for every $j \in I$, such that all the p-powers of these derivations are K-linearly independent. Let $\{E_1, \dots, E_s\}$ be the ordered set $\left\{ D_{1j}^{p^{k_j}} \mid 0 \leq k_j < m_{1j}, j \in I \right\}$. This family satisfies the hypothesis of Proposition 1.2.6 and therefore there exists a p-basis $\{t_1, \dots, t_s\}$ of K/kK^p such that $E_i(t_i) = 1$ and $E_i(t_j) = 0$ for all $j < i$ and $i = 1, \dots, s$. By Lemma 3.2.8, the rational action of G_i is defined on $X^{(p)} \dashrightarrow X/\ker(F_G)$. Notice that the rational isomorphism is a consequence of the fact that both the field extensions $K^{\ker(F_G)} \subseteq K$ and $kK^p \subseteq K$ have degree p^s (in the first case because the rational action of $\ker(F_G)$ on X is generically free and $\ker(F_G)$ has order p^s and in the second case by Proposition 2.1.4) and moreover $kK^p \subseteq K^{\ker(F_G)}$. In particular

$$D_{ij}(F_K(\beta)) = v(T_{ij})(F_K(\beta)) = F_K(v(V_{G_i^\vee}(T_{ij}))(\beta))$$

for every $\beta \in kK^p$. By Lemma 3.2.10, for any $j = 1, \dots, r_i$, we then have that D_{ij} is defined using property 1, provided we choose $x_h^{ij} = D_{ij}(t_h)$ for $h = 1, \dots, s$. Therefore

the first property is respected by definition. We will show that we can choose x_h^{ij} for every h and j in such a way that also properties 2 and 3 are satisfied.

Second recurrence (on j):
We show that if D_{kl} is defined for all $(k,l) <_{LEX} (i,j)$ then we can define D_{ij}. Recall that for the moment D_{ij} is defined on kK^p which is the function field of $X^{(p)}$, so we have that the rational action of G_i is defined on $X^{(p)} \dashrightarrow^{\sim} X/\ker(F_G)$ and we want to extend it to a rational action on X.

Third recurrence (on h):
We will show that if D_{ij} is defined on $kK^p(t_1,\dots,t_{h-1})$, then we can extend its definition to $kK^p(t_1,\dots,t_h)$[1]. The base step is satisfied since D_{ij} is defined on kK^p. We will show that if D_{ij} is defined on $kK^p(t_1,\dots,t_{h-1})$ then the system

$$N_h = \begin{cases} D_{kl}D_{ij}(t_h) = D_{ij}D_{kl}(t_h), & (k,l) <_{LEX} (i,j) \\ D_{ij}^{p^{m_{ij}}}(t_h) = Q_{ij}(D_{k'l'})_{(k',l')<_{LEX}(i,j)}(t_h) \end{cases}$$

has a solution where the unknown is $x_h^{ij} = D_{ij}(t_h)$. Remark that, for the system to admit a solution is equivalent to having properties 2 and 3 satisfied on $kK^p(t_1,\dots,t_h)$. Indeed, by Lemma 3.2.11 and the fact that $P_{ij} = T_{ij}^{p^{m_{ij}}} - Q_{ij}$ is a primitive element, we have that $D_{kl}D_{ij} - D_{ij}D_{kl}$ and $D_{ij}^{p^{m_{ij}}} - Q_{ij}(D_{k'l'})_{(k',l')<_{LEX}(i,j)}$ are derivations. Applying then Remark 1.2.5, we obtain that D_{ij} commutes with D_{kl} for every $(k,l) <_{LEX} (i,j)$ and that $D_{ij}^{p^{m_{ij}}} = v(Q_{ij})$ as claimed. Notice that, in particular, $x_{h'}^{kl} = D_{kl}(t_{h'})$ is a solution of the analogous system for every $(k,l,h') <_{LEX} (i,j,h)$ by the assumption that D_{kl} is defined on K for all $(k,l) <_{LEX} (i,j)$ and that D_{ij} is defined on $kK^p(t_1,\dots,t_{h-1})$. We will first show that the system

$$S_h = \Big\{ D_{kl}D_{ij}(t_h) = D_{ij}D_{kl}(t_h), \quad (k,l) <_{LEX} (i,j)$$

obtained by removing the last equation has a solution and then prove that there exists a solution of it which is also a solution of the last equation of the system N_h. Remark that, for the system S_h to admit a solution is equivalent to having property 2 satisfied on

[1]Geometrically here we are taking a filtration of $\ker(F_G)$ with successive quotients isomorphic to α_p and considering subquotients of X. For example, in the case in which $\ker(F_G) \simeq W_s^1$ with generically free rational action on X given by a derivation D_1 of order p^s, we have the tower

$$K^{D_1} \subseteq K^{D_1^p} = K^{D_1}(t_1) \subseteq \cdots \subseteq K^{D_1^{p^{s-1}}} = K^{D_1}(t_1,\dots,t_{s-1}) \subseteq K = K^{D_1}(t_1,\dots,t_s)$$

corresponding to

$$X \dashrightarrow X/\alpha_p \dashrightarrow X/W_2^1 \dashrightarrow \cdots \dashrightarrow X/W_{s-1}^1 \dashrightarrow X/W_s^1$$

and

$$\alpha_p = \mathrm{soc}(\ker(F_G)) \subseteq W_2^1 = \ker(F_G) \times_k \ker(V_G^2) \subseteq \cdots \subseteq W_{s-1}^1 = \ker(F_G) \times_k \ker(V_G^{s-1}) \subseteq W_s^1 = \ker(F_G).$$

Notice that this phenomenon did not occur in Example 3.2.12 since there the Frobenius kernel was just α_p.

$kK^p(t_1,\dots,t_h)$. First of all, notice that the system S_h is well-defined, that is that D_{ij} is defined on $D_{kl}(t_h)$ for $(k,l) <_{LEX} (ij)$: indeed

$$E_iD_{kl}(t_h) = D_{kl}E_i(t_h) = 0$$

for every $i \geq h$, and thus, by Proposition 1.2.6, $D_{kl}(t_h)$ belongs to $kK^p(t_1,\dots,t_{h-1})$ on which D_{ij} is defined. Let $a_{kl} := D_{ij}D_{kl}(t_h)$, therefore we are looking for a solution of the system

$$S_h = \left\{ D_{kl}(x) = a_{kl}, \quad (k,l) <_{LEX} (i,j). \right.$$

By induction the set $\{D_{kl} \mid (k,l) <_{LEX} (i,j)\}$ is an ordered set of pairwise commuting differential operators and such that D_{kl} is a derivation of order $p^{m_{kl}}$ on the subfield

$$\{a \in K \mid D_{k'l'}(a) = 0 \quad \forall (k',l') <_{LEX} (k,l)\}$$

by Lemma 3.2.8. Moreover,

$$D_{kl}(a_{k'l'}) = D_{k'l'}(a_{kl})$$

for all $(k,l),(k',l') <_{LEX} (i,j)$, indeed by induction

$$D_{kl}D_{k'l'}(t_h) = D_{k'l'}D_{kl}(t_h)$$

and thus

$$D_{kl}(a_{k'l'}) = D_{kl}D_{ij}D_{k'l'}(t_h) = D_{ij}D_{kl}D_{k'l'}(t_h) =$$
$$D_{ij}D_{k'l'}D_{kl}(t_h) = D_{k'l'}D_{ij}D_{kl}(t_h) = D_{k'l'}(a_{kl})$$

as wished. Notice that we used the fact that $D_{kl}(t_h)$ lies in $kK^p(t_1,\dots,t_{h-1})$ and that, by induction, on this subfield D_{ij} commutes with the previous (LEX-order wise) differential operators. In addition, $D_{kl}^{p^{m_{kl}}} = Q_{kl}(D_{k'l'})_{(k',l')<_{LEX}(k,l)}$ where Q_{kl} is an element of $k[T_{k'l'}]_{(k',l')<_{LEX}(k,l)}$ with vanishing constant coefficient. By Corollary 1.2.7, we then know that a solution of the system S_h exists if and only if

$$D_{kl}^{p^{m_{kl}}-1}(a_{kl}) = \widetilde{Q}_{kl}(a_{k'l'})_{(k',l')<_{LEX}(k,l)}$$

for all $(k,l) <_{LEX} (i,j)$. Write the polynomial Q_{kl} as

$$Q_{kl}(T_{k'l'})_{(k',l')<_{LEX}(k,l)} = \sum_{(\alpha,\beta)<_{LEX}(k,l)} \rho_{\alpha\beta}(T_{k'l'})_{(k',l')<_{LEX}(k,l)}T_{\alpha\beta}.$$

Then

$$\widetilde{Q}_{kl}(a_{k'l'})_{(k',l')<_{LEX}(k,l)} = \sum_{(\alpha,\beta)<_{LEX}(k,l)} \rho_{\alpha\beta}(D_{k'l'})_{(k',l')<_{LEX}(k,l)}a_{\alpha\beta} =$$

$$\sum_{(\alpha,\beta)<_{LEX}(k,l)} \rho_{\alpha\beta}(D_{k'l'})_{(k',l')<_{LEX}(k,l)}D_{ij}D_{\alpha\beta}(t_h) =$$

$$D_{ij}\sum_{(\alpha,\beta)<_{LEX}(k,l)} \rho_{\alpha\beta}(D_{k'l'})_{(k',l')<_{LEX}(k,l)}D_{\alpha\beta}(t_h) = D_{ij}Q_{kl}(D_{k'l'})_{(k',l')<_{LEX}(k,l)}(t_h) =$$

$$D_{ij}D_{kl}^{p^{m_{kl}}}(t_h) = D_{kl}^{p^{m_{kl}}-1}D_{ij}D_{kl}(t_h) = D_{kl}^{p^{m_{kl}}-1}(a_{kl})$$

as needed, that is the system S_h admits solution. We are left to show that there exists a solution of S_h that satisfies also the equation

$$D_{ij}^{p^{m_{ij}}-1}(z) = Q_{ij}(D_{k'l'})_{(k',l')<_{LEX}(i,j)}(t_h).$$

Notice that we are looking for a solution of the form

$$x_h^{ij} = x + y$$

with y in

$$K^{\{D_{kl}|(k,l)<_{LEX}(i,j)\}} = \{a \in K \mid D_{kl}(a) = 0 \quad \forall (k,l) <_{LEX} (i,j)\}$$

and x a solution of S_h. Moreover, notice that x lies in $kK^p(t_1,\dots,t_{h-1})$, indeed we remarked that if S_h has solution then D_{ij} commutes with D_{kl} for every $(k,l) <_{LEX} (i,j)$ on $kK^p(t_1,\dots,t_h)$, so in particular it commutes with $E_1,\dots,E_s$ which, we recall, are the p-powers of the derivations D_{1j}, $j \in I$. Hence

$$E_\eta(x) = E_\eta D_{ij}(t_h) = D_{ij}E_\eta(t_h) = 0$$

for all $\eta \geq h$. Therefore $x + y$ is a solution of the equation if and only if

$$D_{ij}^{p^{m_{ij}}-1}(y) = Q_{ij}(D_{k'l'})_{(k',l')<_{LEX}(i,j)}(t_h) - D_{ij}^{p^{m_{ij}}-1}(x).$$

Let us show that the term on the right hand side lies in $K^{\{D_{kl}|(k,l)<_{LEX}(i,j)\}}$. Indeed, for any $(k,l) <_{LEX} (i,j)$ it holds

$$D_{kl}D_{ij}^{p^{m_{ij}}-1}(x) = D_{ij}^{p^{m_{ij}}-1}D_{kl}(x) = D_{ij}^{p^{m_{ij}}-1}D_{ij}D_{kl}(t_h) = D_{ij}^{p^{m_{ij}}}D_{kl}(t_h) =$$

$$Q_{ij}(D_{k'l'})_{(k',l')<_{LEX}(i,j)}D_{kl}(t_h) = D_{kl}Q_{ij}(D_{k'l'})_{(k',l')<_{LEX}(i,j)}(t_h)$$

where we used the fact that $x, D_{kl}(t_h) \in kK^p(t_1,\dots,t_{h-1})$ and that x is a solution of the system S_h. Notice that $K^{\{D_{kl}|(k,l)<_{LEX}(i,j)\}}$ is a subfield of $kK^p = K^{\{D_{1j}|j\in I\}}$ and that D_{ij} is a derivation of order $p^{m_{ij}}$ on $K^{\{D_{kl}|(k,l)<_{LEX}(i,j)\}}$. Therefore, by Lemma 1.2.3, y exists if and only if

$$D_{ij}\left(Q_{ij}(D_{k'l'})_{(k',l')<_{LEX}(i,j)}(t_h) - D_{ij}^{p^{m_{ij}}-1}(x)\right) = 0$$

which is satisfied since

$$D_{ij}^{p^{m_{ij}}}(x) = Q_{ij}(D_{k'l'})_{(k',l')<_{LEX}(i,j)}(x) = \sum_{(\alpha,\beta)<_{LEX}(i,j)} \rho_{\alpha\beta}(D_{k'l'})_{(k',l')<_{LEX}(i,j)}D_{\alpha\beta}(x)$$

$$\sum_{(\alpha,\beta)<_{LEX}(i,j)} \rho_{\alpha\beta}(D_{k'l'})_{(k',l')<_{LEX}(i,j)}D_{ij}D_{\alpha\beta}(t_h) = D_{ij}Q_{ij}(D_{k'l'})_{(k',l')<_{LEX}(i,j)}(t_h),$$

where the first equality is again a consequence of the fact that $x \in kK^p(t_1, \ldots, t_{h-1})$. Notice that the action constructed is generically free since it extends the generically free action of $\mathrm{soc}(G)$ (see Proposition 3.2.1).

For the general case of a variety X of dimension $\dim(X) = \ell \geq s$, consider the infinitesimal commutative unipotent k-group scheme $G \times_k \alpha_p^{\ell-s}$ where $s = \dim_k(\mathrm{Lie}(G))$. Then $\dim_k(\mathrm{Lie}(G \times_k \alpha_p^{\ell-s})) = \ell$ and thus by what we just proved X admits a generically free rational action of $G \times_k \alpha_p^{\ell-s}$. In particular, it admits a generically free rational action of its subgroup G. Moreover, any generically free rational action of $\ker(F_G^r)$ on X extends to a generically free rational action of $\ker(F_G^r) \times_k \alpha_p^{l-s}$ in the following way: consider the set of derivations $\{E_1, \ldots, E_s\}$ defining the action of $\ker(F_G)$ on $K = L(t_1, \ldots, t_s)$ where $L = k(X/\ker(F_G))$ as described in the first part and complete it to a basis $\{E_1, \ldots, E_s, \partial_{s+1}, \ldots, \partial_\ell\}$ where the ∂_i's are as in Remark 1.2.5. One checks easily that the elements of this basis commute pairwise and that this implies that the ∂_i's commute with every differential operator defining the rational action of $\ker(F_G^r)$ on X. By the case treated previously, the rational action of $\ker(F_G^r) \times_k \alpha_p^{l-s}$ extends to a generically free rational action of $G \times_k \alpha_p^{\ell-s}$ and thus, in particular, to a generically free rational action of G. □

Remark 3.2.14. Brion shows that for any $l, n \geq 1$ there exist generically free rational actions of $\mu_{p^l}^n$ on any variety X of dimension $\geq n$ [Bri22, Remark 3.8]. Putting together Brion's result and Theorem 3.2.13 one can prove that if k is perfect and G is an infinitesimal commutative trigonalizable k-group scheme with Lie algebra of dimension s, then for every k-variety X of dimension $\geq s$ there exist generically free rational actions of G on X. Briefly, one considers a set of derivations $\{E_1, \ldots, E_{s_1}\}$ defining a generically free rational action of $\ker(F_{G^u})$ on $K = L(t_1, \ldots, t_{s_1})$ where $L = k(X/\ker(F_{G^u}))$ as described in the first part of the proof of the Theorem and complete it to a K-linearly independent set $\{E_1, \ldots, E_{s_1}, t_{s_1+1}\partial_{s_1+1}, \ldots, t_{s_1+s_2}\partial_{s_1+s_2}\}$, with ∂_i's as in Remark 1.2.5. One checks easily that the elements of this basis commute pairwise and they thus define a generically free rational action of $\ker(F_G)$. Moreover, we can extend it as before to a generically free rational action of $\ker(F_G^r)$ (and so also of G) on X for any $r \geq 1$.

Examples

We conclude this section with some examples to show more concretely how to deal with the construction of actions of infinitesimal group schemes.

Example 3.2.15. Let $G = W_2^2[F - V] = \mathrm{Spec}\left(k[S_0, S_1]/(S_0^p, S_1^p - S_0)\right)$. We aim to show that we can construct naturally a generically free G-action on a curve. Notice that G is a k-subgroup scheme of $W_2^2 = \mathrm{Spec}\left(k[T_0, T_1]/(T_0^{p^2}, T_1^{p^2})\right)$ and that we have a natural action of W_2^2 on $W_2 \simeq \mathbb{A}_k^2$ given by translation, that is

$$\begin{aligned} &\rho : W_2^2 \times_k \mathbb{A}_k^2 \to \mathbb{A}_k^2 \\ &((a,b),(x,y)) \mapsto (a + x, b + y + S_1(a,x)) \end{aligned}$$

where $S_1(a,x) = -\sum_{j=1}^{p} \frac{1}{p}\binom{p}{j} a^j x^{p-j}$. We then have an induced action of G on $\mathbb{A}^2_k$ given by

$$((b^p,b),(x,y)) \mapsto (b^p + x, b + y + S_1(b^p,x)).$$

Consider now the affine line given by $\operatorname{Spec}(k[x,y]/(y^p - x)) \simeq \mathbb{A}^1_k$ inside $\mathbb{A}^2_k$. The restriction of ρ to $G \times_k \mathbb{A}^1_k$ induces an action of G on $\mathbb{A}^1_k$: indeed

$$(b + y + S_1(b^p,x))^p = b^p + y^p + S_1(b^{p^2}, x^p) = b^p + x$$

where we used the fact that $b^{p^2} = 0$. This provides us in a natural way with a generically free action of G on a curve.

Let us now show how to express these actions in terms of differential operators, that is show which are the corresponding module algebra structures. Let $A = k[T_0,T_1]/(T_0^{p^2}, T_1^{p^2})$, then ρ corresponds to the coaction

$$\begin{aligned} k[x,y] &\to A \otimes_k k[x,y] \\ x &\mapsto T_0 \otimes 1 + 1 \otimes x, \\ y &\mapsto T_1 \otimes 1 + 1 \otimes y + S_1(T_0 \otimes 1, 1 \otimes x) \end{aligned}$$

and the associated $A^\vee$-module algebra structure on $k[x,y]$ is given by

$$\begin{aligned} v : A^\vee &\to \operatorname{Diff}_k(k[x,y]) \\ \varphi &\mapsto (k[x,y] \xrightarrow{\rho} A \otimes_k k[x,y] \xrightarrow{\varphi \otimes \mathrm{id}} k \otimes_k k[x,y] \simeq k[x,y]) \end{aligned}$$

(see Proposition 3.1.17). Now $A^\vee$ is isomorphic to A, where the isomorphism is given by

$$\begin{aligned} T_0^* &\mapsto T_0, \\ T_1^* &\mapsto T_0^p, \\ (T_0^p)^* &\mapsto T_1, \\ (T_1^p)^* &\mapsto T_1^p. \end{aligned}$$

We then see that $v(T_0)(x) = 1$ and $v(T_0)(y) = -x^{p-1}$, implying that $v(T_0) = \partial_x - x^{p-1}\partial_y$. Similarly we obtain that $v(T_1) = \partial_{x^p} - (x^p)^{p-1}\partial_{y^p}$. The invariants of this action are given by $\operatorname{Spec}\left(k[x^{p^2}, y^{p^2}]\right)$. The module algebra structure corresponding to the action of G on $\mathbb{A}^2_k$ is obtained by considering the composite

$$k[G]^\vee \hookrightarrow A^\vee \xrightarrow{v} \operatorname{Diff}_k(k[x,y]).$$

The group scheme G is also self-dual and the inclusion is given by

$$\begin{aligned} S_0 &\mapsto T_0^p, \\ S_1 &\mapsto T_1^p + T_0. \end{aligned}$$

We thus obtained that the $k[G^\vee]$-module algebra on $k[x,y]$ is defined by

$$v(S_0) = v(T_0)^p = \partial_y \quad \text{and} \quad v(S_1) = v(T_1)^p + v(T_0) = \partial_{y^p} + \partial_x - x^{p-1}\partial_y$$

and the invariants are $\mathrm{Spec}\,(k[x^p, x+y^p])$. If we restrict to $\mathbb{A}^1_k \simeq \mathrm{Spec}\,(k[x,y]/(y^p-x))$, the module algebra structure is given by $v(S_1) = \partial_{y^p} - (y^p)^{p-1}\partial_y$ and its invariants are $\mathrm{Spec}(k[y^p])$.

Example 3.2.16. Consider the k-group scheme

$$G = W_2^3[F^2 - V] = \mathrm{Spec}\left(k[T_0, T_1]/(T_0^p, T_1^{p^2} - T_0)\right).$$

It has one-dimensional Lie algebra so by Theorem 3.2.13 we know that we can find a generically free rational action of G on any curve. Its dual is the k-group scheme

$$G^\vee = W_3^2[F - V^2] = \mathrm{Spec}\,(k[U_0, U_1, U_2]/(U_0^p, U_1^p, U_2^p - U_0))$$

where $U_0 = T_1^*, U_1 = (T_1^p)^*, U_2 = T_0^*$. Notice that $G \times_k G^\vee$ is the p-torsion of an abelian variety of dimension 3 with p-rank 0 and a-number 2 (see [Pri08] where this group scheme is denoted $I_{3,2}$). The filtration of G given by the kernel of the Frobenius powers, $G_i = \ker(F_G^i)$, is

$$G_1 = \mathrm{Spec}\,(k[T_1]/(T_1^p)) \subseteq G_2 = \mathrm{Spec}\left(k[T_1]/(T_1^{p^2})\right) \subseteq G$$

corresponding to the cofiltration

$$G^\vee \twoheadrightarrow G_2^\vee = \mathrm{Spec}\,(k[U_0, U_1]/(U_0^p, U_1^p)) \twoheadrightarrow G_1^\vee = \mathrm{Spec}\,(k[U_0]/(U_0^p)) \twoheadrightarrow 0$$

where $G_i^\vee = \mathrm{coker}(V_{G^\vee}^i)$. A generically free rational action of G on a curve with function field $K = kK^p(t)$ is given for example by

$$\begin{aligned} U_0 &\mapsto \partial_t, \\ U_1 &\mapsto \partial_{t^p}, \\ U_2 &\mapsto \partial_{t^{p^2}} - \left(t^{p^2}\right)^{p-1}\partial_t. \end{aligned}$$

Say now that we want to study rational actions of $G^\vee$. Notice that its Lie algebra has dimension 2, hence we know that we can find a generically free rational action of $G^\vee$ on any k-variety of dimension at least 2 (but not on curves). The filtration of $G^\vee$ given by the kernel of Frobenius powers is now

$$\mathrm{Spec}\,(k[U_1, U_2]/(U_1^p, U_2^p)) \subseteq G^\vee$$

and corresponds to the cofiltration

$$G \twoheadrightarrow \mathrm{Spec}\left(k[T_0, T_1^p]/(T_0^p, T_1^{p^2} - T_0)\right) \twoheadrightarrow 0.$$

If we denote by $V_0 = T_1^p$ we have $G \twoheadrightarrow \mathrm{Spec}\left(k[V_0]/(V_0^{p^2})\right)$ and

$$k[G] = k[V_0, T_1]/(V_0^{p^2}, T_1^p - V_0)$$

where the comultiplication is

$$V_0 \mapsto V_0 \otimes 1 + 1 \otimes V_0,$$
$$T_1 \mapsto T_1 \otimes 1 + 1 \otimes T_1 + S_1(V_0^p \otimes 1, 1 \otimes V_0^p).$$

A generically free rational action of $G^\vee$ on a k-surface with function field $K = kK^p(x,y)$ is given for example by

$$V_0 \mapsto D_0 = \partial_x - x^{p-1}\partial_y,$$
$$T_1 \mapsto \partial_{y^p} - (y^p)^{p-1}(D_0 + (y^{p^2})^{p-1}D_0^p).$$

Example 3.2.17. Let $k = \overline{k}$ be a field of characteristic 2, E be a supersingular elliptic curve over k and consider its 2-torsion

$$E[2] = \mathrm{Spec}\left(k[T_0,T_1]/(T_0^2, T_1^2 - T_0)\right)$$

(see Corollary 2.3.10). The k-group scheme $E[2]$ is self-dual, that is

$$E[2]^\vee = \mathrm{Spec}(k[U_0,U_1]/(U_0^2, U_1^2 - U_0))$$

where $U_0 = T_1^*$ and $U_1 = T_0^*$. We are interested in studying actions of $E[2]$ on $\mathbb{P}^1_k$. By Theorem 3.2.13 and by the assumption on the characteristic, all the generically free rational actions of $E[2]$ on $\mathbb{P}^1_k$ are given by

$$\begin{aligned} v : k[U_0,U_1]/(U_0^2, U_1^2 - U_0) &\mapsto \mathrm{Diff}_k(k(t)) \\ U_0 &\mapsto \partial_t, \\ U_1 &\mapsto \partial_{t^2} + (t^2 + g(t^4))\partial_t \end{aligned}$$

corresponding to

$$\begin{aligned} \rho : E[2] \times_k \mathbb{P}^1_k &\dashrightarrow \mathbb{P}^1_k \\ (a,t) &\mapsto t + a + (t^2 + g(t^4))a^2 \end{aligned}$$

where $g \in k(t)$. Which of these rational actions extend to a regular action of $E[2]$ on $\mathbb{P}^1_k$? First of all, if we want ρ to be defined on $\mathbb{A}^1_k = \mathrm{Spec}(k[t])$ we need for g to lie in $k[t]$. Let us now show that ρ extends to an action on $\mathbb{P}^1_k$ if and only if g is constant. Notice that

$$\left(t + a + (t^2 + g(t^4))a^2\right)^4 = (t^2 + a^2)^2 = t^4$$

and thus

$$\left(t + a + (t^2 + g(t^4))a^2\right)^{-1} = \frac{1}{t^4}(t + a + (t^2 + g(t^4))a^2)(t^2 + a^2) =$$

$$\frac{1}{t} + \frac{a}{t^2} + \left(1 + \frac{g(t^4)}{t^2} + \frac{a^2}{t^3}\right)a^2 + \frac{a^3}{t^4}.$$

Hence

$$\left(a, \frac{1}{t}\right) \mapsto \frac{1}{t} + \frac{a}{t^2} + \left(1 + \frac{g(t^4)}{t^2} + \frac{a^2}{t^3}\right) a^2 + \frac{a^3}{t^4}$$

which defines an action on $\mathbb{A}^1_k = \operatorname{Spec}\left(k\left[\frac{1}{t}\right]\right)$ if and only if g is constant. Recall that for A a local k-algebra, the exact sequence of group schemes

$$1 \to \mathbb{G}_{m,k} \to \mathrm{GL}_{2,k} \to \mathrm{PGL}_{2,k} \to 1$$

yields the short exact sequence of groups

$$1 \to \mathbb{G}_{m,k}(A) \to \mathrm{GL}_{2,k}(A) \to \mathrm{PGL}_{2,k}(A) \to 1,$$

that is every element of $\mathrm{PGL}_{2,k}(A)$ is represented by a matrix in $\mathrm{GL}_{2,k}(A)$. The action $E[2] \to \mathrm{Aut}_{\mathbb{P}^1_k} \simeq \mathrm{PGL}_{2,k}$ given by $t \mapsto t + a + (t^2 + c)a^2$ corresponds to a point of $\mathrm{PGL}_{2,k}(E[2])$ and is therefore represented by a matrix which is

$$\begin{pmatrix} 1 + \sqrt{c}a^2 & a^2 \\ a + ca^2 + \sqrt{c}a^3 & 1 + \sqrt{c}a^2 + a^3 \end{pmatrix}.$$

Indeed

$$\frac{(1 + \sqrt{c}a^2)t + a + ca^2 + \sqrt{c}a^3}{a^2t + 1 + \sqrt{c}a^2 + a^3} = ((1 + \sqrt{c}a^2)t + a + ca^2 + \sqrt{c}a^3)(a^2t + 1 + \sqrt{c}a^2 + a^3) =$$

$$t(a^2t + 1 + \sqrt{c}a^2 + a^3) + \sqrt{c}a^2t + a^3t + a + \sqrt{c}a^3 + ca^2 + \sqrt{c}a^3 =$$

$$a^2t^2 + t + a + ca^2 = t + a + (t^2 + c)a^2.$$

Notice that we showed that in characteristic 2 the 2-torsion $E[2]$ of a supersingular elliptic curve is a subgroup scheme of $\mathrm{PGL}_{2,k}$ (its subgroup schemes will be more thoroughly studied in the last section of this chapter). On the other hand, in characteristic $p > 2$ no rational action of $E[p]$ on $\mathbb{P}^1_k$ extends to a regular action, indeed in this case every infinitesimal subgroup scheme of $\mathrm{PGL}_{2,k}$ lifts to $\mathrm{GL}_{2,k}$ (see Proposition 3.4.4) and, in particular, the infinitesimal commutative unipotent subgroup schemes of $\mathrm{PGL}_{2,k}$ are all isomorphic to α_{p^n} for some $n \geq 1$.

The following example (which is also an example of a subgroup scheme of $\mathrm{PGL}_{2,k}$ in the particular case $p = 2$ and $n = 3$, see Theorem 3.4.1) goes in the direction of studying also generically free rational actions on curves of non-commutative group schemes.

Example 3.2.18. Consider the infinitesimal unipotent non-commutative k-group scheme $G = \operatorname{Spec}(A)$ of Example 2.3.13 where

$$A = k[T_0, T_1] / \left(T_0^{p^n}, T_1^p - T_0\right)$$

with $n \geq 2$ an integer and comultiplication given by

$$\Delta(T_0) = T_0 \otimes 1 + 1 \otimes T_0$$

and

$$\Delta(T_1) = T_1 \otimes 1 + 1 \otimes T_1 + T_0^{p^{n-1}} \otimes T_0^{p^{n-2}}.$$

Recall that in this case

$$A^\vee =$$

$$k\langle U_0 \dots, U_n\rangle/(U_0^p, \dots, U_n^p, U_iU_j - U_jU_i, U_nU_{n-1} - U_{n-1}U_n - U_0)_{i,j=0,\dots n,(i,j),(j,i)\neq(n,n-1)}$$

where $U_0(T_1) = 1$ and $U_i(T_0^{p^{i-1}}) = 1$ and zero elsewhere. The Hopf algebra $A^\vee$ is non-commutative: the only non-commutative relation is given by $U_nU_{n-1} - U_{n-1}U_n = U_0$, while its comultiplication is defined on the U_i's as for the Witt vectors (notice that this makes sense since $U_0, \dots, U_{n-1}$ commute). Let X/k be a curve and $K = k(X) = kK^p(t)$ be its function field, for t a p-generator of K over kK^p. A generically free rational action of G on X is given by defining an $A^\vee$-module algebra structure on K setting $v(U_i) = D_i = \partial_{p^i}$ for $i = 0, \dots, n-1$ and $v(U_n) = D_n = \partial_{p^n} - t^{p^{n-1}}\partial_1$. Notice that $\partial_{p^n}(t^{p^{n-1}}) = 0$ and thus ∂_{p^n} commutes with $t^{p^{n-1}}\partial_1$. Therefore

$$D_n^p = \partial_{p^n}^p - (t^{p^{n-1}}\partial_1)^p = \partial_{p^n}^p - t^{p^n}\partial_1^p = 0$$

where for the second equality we used that also $\partial_1(t^{p^{n-1}}) = 0$ and for the last that $\partial_{p^n}^p = \partial_1^p = 0$. Of course this rational action can be extended to a generically free rational action of G on any variety of positive dimension.

3.3 Faithful rational actions

This section is devoted to Dolgachev's conjecture revisited for infinitesimal group schemes and more generally to studying faithful rational actions of infinitesimal group schemes. Dolgachev made the following conjecture for the Cremona group over a field of positive characteristic.

Conjecture. If k is a field of characteristic $p > 0$, the Cremona group $\mathrm{Cr}_n(k)$ does not contain elements of order p^s for $s > n$ [Dol10, Conjecture 37].

The conjecture is true for $n = 1$ since $\mathrm{PGL}_2(k) \simeq \mathrm{Aut}_k(k(t))$ does not contain elements of order p^2 if $char(k) = p > 0$. Moreover, it was proven for $n = 2$ [Dol09]. The conjecture can be rephrased in the following way: if there exists a faithful rational action of a finite commutative p-group G on $\mathbb{P}_k^n$ then $p_G^n = 0$, where p_G is the multiplication by p morphism on G. Indeed there is a natural correspondence between faithful actions of a finite group G on $k(t_1, \dots, t_n)$ and faithful rational actions of the corresponding constant group scheme on $\mathbb{P}_k^n$. In fact, an action $G \times k(t_1, \dots, t_n) \to k(t_1, \dots, t_n)$ can be extended naturally to a $k[G]$-module algebra structure $k[G] \to \mathrm{End}_k(k(t_1, \dots, t_n))$, where $k[G]$ is the group algebra over G with its Hopf algebra structure (see also Example 1.1.15) and this gives a faithful rational action of the constant group scheme G on $\mathbb{P}_k^n$. The analogous of Dolgachev's conjecture in our context is given by Proposition 3.3.6, that we will now prove after a couple of preliminary results.

Proposition 3.3.1. *Let G be a finite k-group scheme and X a k-scheme endowed with a G-action. The action is faithful if and only if the induced action of* $\mathrm{soc}(G)$ *is faithful.*

Proof. The G-action is faithful if and only if the centralizer $C_G(X)$ is trivial. By Lemma 2.2.19, since $C_G(X)$ is a normal k-subgroup scheme of G, the centralizer is trivial if and only if $\mathrm{soc}(G) \times_G C_G(X) = C_{\mathrm{soc}(G)}(X)$ is trivial, that is if and only if the induced $\mathrm{soc}(G)$-action is faithful. □

The following result generalizes [Bri22, Lemma 5.3].

Corollary 3.3.2. *Let G be an infinitesimal commutative k-group scheme, acting rationally on a k-variety X. Then the rational G-action is generically free if and only if it is faithful and the induced action of* $\mathrm{soc}((G_{\overline{k}})^u)$ *is generically free, where $(G_{\overline{k}})^u$ is the maximal unipotent subgroup scheme contained in $G_{\overline{k}}$. In particular, if* $\mathrm{soc}((G_{\overline{k}})^u) \subseteq \alpha_p$*, then the G-action is faithful if and only if it is generically free.*

Proof. By Lemma 3.1.4 and Proposition 3.1.10, we may suppose $k = \overline{k}$. The *only if* part is clear. We prove the other implication. We first prove the case G diagonalizable. In this case, we have to prove that if the G-action is faithful then it is generically free. By the anti-equivalence of categories between diagonalizable group schemes and abelian groups, if the stabilizer of the generic point $\mathrm{Spec}(K)$ of X is not trivial over K, then it comes from a non-trivial subgroup of G over k, which then acts trivially, meaning that the action is not faithful.

Now we pass to the general case. Since $k = \overline{k}$ then G is isomorphic to $G^u \times_k G^d$, where G^d is diagonalizable. Since the $\mathrm{soc}(G^u)$-action is generically free, the stabilizer at the generic point $\mathrm{Spec}(K)$ should be contained in G^d_K, but this is not possible since the G^d-action is generically free by the diagonalizable case. For the last sentence we observe that if $\mathrm{soc}(G^u)$ is a subgroup scheme of α_p and the G-action is faithful, then the $\mathrm{soc}(G^u)$-action is generically free. So we can apply the first part of the corollary. □

Remark 3.3.3. The above Corollary applies, for instance, to any infinitesimal subgroup scheme G of W_n, for some n: indeed in this case $\mathrm{soc}(G) = \alpha_p$ (see Example 2.2.28).

In the following corollary we essentially get the second part of [Bri22, Lemma 3.7]

Corollary 3.3.4. *Let G be an infinitesimal k-group scheme acting faithfully on a k-variety of dimension r. If H is a normal k-subgroup scheme of G of multiplicative type such that* $\dim_k(\mathrm{Lie}(H)) = r$*, then G is of multiplicative type and* $\dim_k(\mathrm{Lie}(G)) = r$*.*

Proof. By [DG70, IV, §1, Corollary 4.4] we have that H is central in G. Now we can suppose that k is algebraically closed, then H is diagonalizable. If G is not diagonalizable then G contains a k-subgroup scheme isomorphic to α_p ([DG70, IV §3, Lemma 3.7]). Then $H' = H \times_k \alpha_p$ is contained in G since H is central. Now H' is commutative, $\mathrm{soc}(H') = \ker F_H \times_k \alpha_p$ and $\mathrm{soc}((H')^u) = \alpha_p$. Therefore, by Corollary 3.3.2, the action of H' is generically free, but this is impossible since $\dim_k(\mathrm{Lie}(H')) > r$. So G is diagonalizable, its action is generically free (again by Corollary 3.3.2), and $\dim_k(\mathrm{Lie}(G))$ can not be bigger than r. □

Example 3.3.5. The condition on the normality of H is crucial. Consider for example the k-group scheme $G = \alpha_p \rtimes \mu_p$ (where the action of μ_p on α_p is given by multiplication on the left) and the action on the affine line $G \times_k \mathbb{A}^1_k \to \mathbb{A}^1_k$ given by $(a, b) \cdot x \mapsto ax + b$. The G-action is faithful but not generically free (see Proposition 3.1.15). The stabilizer of the generic point η is

$$\mathrm{Stab}_G(\eta) = \mathrm{Spec}\,(k(x)[T, 1/T, S]/(xT + S - x, T^p - 1, S^p))$$

with comultiplication given by $\Delta(T) = T \otimes T$ and $\Delta(S) = S \otimes 1 + T \otimes S$. This is also a counterexample to Corollary 3.3.2 in the non-commutative case. Indeed $\mathrm{soc}(G) = \alpha_p$ and α_p acts freely. It is then necessary, in the non-commutative case, to look at the action of $\ker(F_G)$, as seen in the first statement of Proposition 3.2.1.

Proposition 3.3.6. *Let G be an algebraic k-group scheme with commutative Frobenius kernel and X be a k-variety of dimension n. If there exists a faithful rational G-action on X, then $s = dim_k(\mathrm{Lie}(\ker(F_G)^m)) \leq n$ and $V^{n-s}_{\ker(F_G)^u} = 0$, where $\ker(F_G)^m$ is the maximal k-subgroup scheme of multiplicative type of $\ker(F_G)$ and $\ker(F_G)^u := \ker(F_G)/\ker(F_G)^m$.*

Proof. We may suppose that G is infinitesimal of height one and that k is algebraically closed. Then

$$G \simeq G^u \times_k G^m = \prod_{i \in I} W^1_{n_i} \times_k \mu^s_p.$$

Clearly $s = \dim_k(\mathrm{Lie}(G^m)) \leq n$ since a faithful rational μ^s_p-action is generically free. Let $l = \max_{i \in I}\{n_i\}$. By Corollary 3.3.2 the induced faithful rational action of $W^1_l \times_k \mu^s_p$ on X is generically free. Hence $l + s \leq n$ and thus $V^{n-s}_{G^u} = 0$. □

Notice that if k is a perfect field, then the above Proposition tells us that if G is an infinitesimal commutative trigonalizable k-group scheme such that there exists a faithful rational G-action on a k-variety of dimension n, then $\ker(F_G)^u \subseteq \left(W^1_{n-s}\right)^l$ for some $l \geq 1$ where $s = \dim_k(\mathrm{Lie}(G^d))$. In particular, if there exists a faithful rational G-action on a curve, then $\ker(F_G)^u \subseteq \alpha^l_p$ for some $l \geq 1$. The converse implication of Proposition 3.3.6 does not always hold true. In the diagonalizable case, these actions are well understood and the converse statement is known. Notice that by Remark 3.2.14 the converse of Proposition 3.3.6 holds as well, over a perfect field, for infinitesimal commutative trigonalizable k-group schemes with Lie algebra of dimension upper bounded by the dimension of X. In particular, if $s = \dim_k(\mathrm{Lie}(\ker(F_G)^d))$ and $\dim_k(\mathrm{Lie}(G)) \leq n$, then $V^{n-s}_{\ker(F_G)^u} = 0$. We will now give a counterexample to the converse implication of Proposition 3.3.6: we exhibit an infinitesimal commutative unipotent k-group scheme G such that $V_{\ker(F_G)} = 0$ but for which there are no faithful rational G-actions on any curve. We then keep investigating other cases in which the converse of Proposition 3.3.6 holds.

Example 3.3.7. Consider the k-subgroup scheme G of $W_2 \times_k W_2$ represented by the Hopf algebra

$$k[T_0, T_1, U_0, U_1]/(T^p_0, T^p_1 - T_0, U^p_0, U^p_1 - U_0).$$

The group scheme G is self-dual and, if k is algebraically closed, $G \simeq E[p] \times_k E[p]$ for E a supersingular elliptic curve over k (that is G is the p-torsion of a superspecial abelian surface). Moreover, $\dim_k(\mathrm{Lie}(G)) = 2$ and $V_{\ker(F_G)} = 0$. Therefore, by Proposition 3.1.15, we know that there is no generically free rational G-action on any curve. Let us show that moreover there is no faithful rational G-action on any curve either. Let X be a curve and $K = k(X)$ be its function field. Suppose that there exists a faithful rational G-action on X defined by the module algebra structure

$$v : k[T_0, T_1, U_0, U_1]/(T_0^p, T_1^p - T_0, U_0^p, U_1^p - U_0) \to \mathrm{Diff}_k(K).$$

The differential operator $v(T_0)$ is a derivation on K of order p, thus, by Lemma 1.2.3, there exists $x \in K$ such that $v(T_0)(x) = 1$. Then, $v(T_0) = \partial_x$, the only k-linear derivation on $K = kK^p(x)$ such that $\partial_x(x) = 1$. As a consequence, $v(U_0) = f_1\partial_x$ for some $f_1 \in K$ since $\mathrm{Der}_k(K)$ is one-dimensional over K. Moreover, f_1 lies in kK^p since the $v(T_0)$ and $v(U_0)$ commute, and is non-constant since the action is faithful and thus $v(T_0)$ and $v(U_0)$ must be k-linearly independent. Now, $v(T_1)(x) = x_1$ for some $x_1 \in kK^p$, since $v(T_1)$ commutes with ∂_x. Moreover $v(T_1)_{|kK^p}$ is a derivation of order p and $v(T_1)(x^p) = (v(T_0)(x))^p = 1$ (see Remark 3.2.9). The differential operator $v(T_1)$ commutes also with $v(U_0) = f_1\partial_x$, hence

$$v(T_1)(f_1) = f_1\partial_x(x_1) = 0$$

that is f_1 must lie in kK^{p^2}. Moreover, x_1 is such that

$$v(T_1)^{p-1}(x_1) = v(T_1^p)(x) = v(T_0)(x) = 1.$$

Consider now $v(U_1)$: as before, $v(U_1)(x) = x_2$ for some $x_2 \in kK^p$ because of the commutativity with ∂_x, $v(U_1)_{|kK^p}$ is a derivation of order p and by Remark 3.2.9 we have $v(U_1)(x^p) = (v(U_0)(x))^p = f_1^p$. Hence $v(U_1)_{|kK^p} = f_1^p v(T_1)_{|kK^p}$. The differential operator $v(U_1)$ commutes also with $v(T_1)$, thus

$$v(T_1)(x_2) = v(T_1)v(U_1)(x) = v(U_1)v(T_1)(x) = v(U_1)(x_1) = f_1^p v(T_1)(x_1) = v(T_1)(f_1^p x_1).$$

Finally,

$$f_1 = v(U_0)(x) = v(U_1^p)(x) = (f_1^p)^{p-1}v(T_1)^{p-1}(x_2) =$$
$$(f_1^p)^{p-1}v(T_1)^{p-1}(f_1^p x_1) = f_1^{p^2}v(T_1)^{p-1}(x_1) = f_1^{p^2}$$

and this condition contradicts the fact that f_1 had to be non constant. Therefore there is no faithful rational G-action on any curve. Notice that we nevertheless showed that there exist faithful rational actions on any curve of the subgroup scheme H of G represented by the Hopf subalgebra

$$k[T_0, T_1, U_1]/(T_0^p, T_1^p - T_0, U_1^p),$$

that is $H \simeq E[p] \times_k \alpha_p$ over $k = \overline{k}$. Actually, this kind of behaviour takes always place as shown in the following result.

The following Proposition generalizes a result of Brion [Bri22, Lemma 3.6] stating that every variety of positive dimension admits a faithful rational action of α_p^ℓ for any $\ell \geq 1$.

Proposition 3.3.8. *Let k be perfect, G be an infinitesimal commutative unipotent k-group scheme and X be a k-variety of dimension n. If $\dim_k(\mathrm{Lie}(G)) \leq n$, then for every $\ell \geq 0$ there exists a faithful rational action of $G \times_k \ker(F_G)^\ell$ on X.*

Proof. Let $s = \dim_k(\mathrm{Lie}(G))$ and $K = k(X)$ be the function field of X. Then $\ker(F_G)$ corresponds to a certain Young diagram $(m_1, \ldots, m_h)$ for some $h \geq 1$, $\sum_{i=1}^h m_i = s$ and $\ker(F_G)^\vee \simeq \prod_{i=1}^h \alpha_{p^{m_i}}$. We know (Proposition 3.2.4) that there exist generically free rational actions of $\ker(F_G)$ on X. By [DG70, III.§2, Corollary 2.7], to give such a rational action corresponds to giving a set of derivations $\{D_1, \ldots, D_h\}$ on K commuting pairwise, with D_i of order p^{m_i} for every $i = 1, \ldots, h$ and such that all the p-powers of these derivations are K-linearly independent. Moreover, by Theorem 3.2.13 this action can be extended to a generically free rational G-action on X. Let $L = K^G$ be the function field of X/G. Take non-constant k-linearly independent elements

$$\{f_{i1}, \ldots, f_{ih} \mid i = 1, \ldots, \ell\}$$

in L. Then $\{f_{i1}D_1, \ldots, f_{ih}D_h\}$ is still a set of derivations defining a generically free rational action of $\ker(F_G)$ on X. Consider then the induced rational action of $G \times_k \ker(F_G)^\ell$ on X and notice that it is faithful by Proposition 3.3.1. Indeed the rational action of $\ker(F_{G \times_k \ker(F_G)^\ell}) = \ker(F_G)^{\ell+1}$ is given by the set of derivations

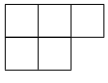
$$\{D_1, \ldots, D_h, f_{i1}D_1, \ldots, f_{ih}D_h \mid i = 1, \ldots, l\}$$

whose p-powers are k-linearly independent and thus it is faithful. □

Remark 3.3.9. Notice that as a direct consequence we have that for any infinitesimal commutative unipotent k-group scheme G of height one, there exist faithful rational G^ℓ-actions on any k-variety of dimension $\geq \dim_k(\mathrm{Lie}(G))$ for any $\ell \geq 1$. In the proof we actually prove something more. Indeed we construct a faithful rational action of G^ℓ such that the induced action of any copy of G is generically free.

Proposition 3.3.10. *Let k be perfect, G be an infinitesimal commutative unipotent k-group scheme and X be a k-variety of dimension n. If $V_G^n = 0$ then there exists a faithful rational G-action on X.*

Proof. It is enough to prove that there exists a faithful rational action of $(W_n^m)^r$ on X for any $m, r \geq 1$. By Proposition 3.2.4, there exist generically free rational actions of W_n^m on X for any $m \geq 1$ and to give such an action corresponds to giving a set of differential operators $\{D_0, \ldots, D_{m-1}\}$ on the function field $k(X)$ of X commuting pairwise, with D_i of order p^i and p^n-nilpotent ($D_i^{p^{n-1}} \neq 0$) for every $i = 0, \ldots, m-1$. Let L be the function field of X/W_n^m. Take k-linearly independent elements $\{f_1, \ldots, f_r\}$ in L. Then $\left\{f_i D_0, f_i^p D_1, \ldots, f_i^{p^{m-1}} D_{m-1} \mid i = 1, \ldots, r\right\}$ gives a faithful rational action of $(W_n^m)^r$ on X. Indeed, since we took the $f_i's$ in L, these differential operators all commute pairwise and are moreover p^n-nilpotent. In addition, by the weighted homogeneity of Witt vectors, they respect the property of compatibility with products. Finally, the action is faithful because the action of the Frobenius kernel is faithful, since we chose $f_1, \ldots, f_r$ linearly independent over k. □

Recall from Chapter 2 that if we take $G_1, \dots, G_l$ commutative unipotent k-group schemes of height one, there exists a smallest commutative unipotent k-group scheme G of height one containing all of them. Precisely, G corresponds to the smallest Young diagram containing all the Young diagrams $\tau(G_i)$ for all i. Explicitly, if $\tau(G_i) = (n_{1i}, \dots, n_{s_i i})$ for some $s_i \geq 1$ and for $i = 1, \dots, l$ then $\tau(G) = (n_1, \dots, n_s)$ where $s = \max\{s_1, \dots, s_l\}$ and $n_j = \max\{n_{j1}, \dots, n_{jl}\}$ for every $j = 1, \dots, s$. For example, if we take $G_1 = W_3^1 \times_k \alpha_p$ and $G_2 = W_2^1 \times_k W_2^1$, then $\tau(G) =$  and $G = W_3^1 \times_k W_2^1$.

Using this, we obtain a sort of converse of Proposition 3.3.8 in the case of group schemes of height one. The following Proposition shows that if $G_1 \times_k \cdots \times_k G_l$ acts on a variety X and the action restricted to every G_i is generically free, then there exists a generically free G-action on X.

Proposition 3.3.11. *Let k be perfect, $H = \prod_{i=1}^{l} G_i$ be an infinitesimal commutative unipotent k-group scheme of height one and X be a k-variety of dimension n. Then there exists a faithful rational H-action on X which induces generically free G_i-actions for every $i = 1, \dots, l$ if and only if there exists an infinitesimal commutative unipotent k-group scheme G of height one such that $\dim_k(\mathrm{Lie}(G)) \leq n$ and $G_i \hookrightarrow G$ for all $i = 1, \dots, l$.*

Proof. The 'if' part is clear by Remark 3.3.9. Suppose now that there exists a faithful rational H-action on X which induces generically free G_i-actions for every $i = 1, \dots, l$ and let K denote the function field of X. By assumption, every G_i is of height one and thus corresponds to a Young diagram $\tau(G_i) = (n_{1i}, \dots, n_{s_i i})$ for some $s_i \geq 1$ and $n_{s_i i} \neq 0$. Recall that s_i corresponds to the length of the first column of $\tau(G_i)$, that is $\dim_k(\mathrm{Lie}(\mathrm{soc}(G_i))$ (see Lemma 2.2.29). The H-action is determined by a set of derivations D_{ji}, with $i = 1, \dots l$ and $j = 1, \dots, s_i$, such that they commute pairwise and $D_{ji}^{p^{n_{ji}}} = 0$. The fact that each G_i-action is generically free is equivalent to the fact that

$$S_i = \left\{ D_{ji}^{p^{n_{ji}-1}} \mid j = 1, \dots, s_i \right\}$$

is linearly independent over K for any $i = 1, \dots, l$. Indeed S_i represents the action induced by $\mathrm{soc}(G_i)$. Let G be the smallest infinitesimal commutative unipotent group scheme of height one containing G_i for all i. Then $\tau(G) = (n_1, \dots, n_s)$ where $s = \max\{s_1, \dots, s_l\}$ and $n_j = \max\{n_{j1}, \dots, n_{jl}\}$ for every $j = 1, \dots, s$. We also fix a function

$$f : \{1, \dots, s\} \mapsto \{1, \dots, l\}$$

such that $n_j = n_{jf(j)}$. This means that for the j-th line of the Young diagram of G we are choosing the j-th line of $G_{f(j)}$. Now we want to construct an action of G on X, or equivalently a set of derivations E_i which commute pairwise and such that $E_i^{p^{n_i}} = 0$ for any $i = 1, \dots, s$. We define $E_1 := D_{1f(1)}$. Now suppose we have defined E_r, with $1 \leq r \leq s-1$, such that the set

$$C_r = \left\{ E_k^{p^{n_k - 1}} \mid k = 1, \dots, r \right\}$$

is linearly independent over K, then we define E_{r+1} in such way that it does not belong to the space generated by C_r. We remark that $\tau(G_{f(r+1)})$ has at least $r+1$ lines which have at least n_{r+1} squares. Now

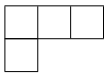
$$\left\{ D_{kf(r+1)}^{p^{n_k}-1} \mid k = 1, \ldots, r+1 \right\}$$

is a set of $r+1$ K-linearly independent derivations, therefore there exists $k_0 \in \{1, \ldots, r+1\}$ such that $D_{k_0 f(r+1)}^{p^{n_{k_0}}-1}$ does not belong to the K-vector space generated by C_r. We define $E_{r+1} := D_{k_0 f(r+1)}^{p^{n_{k_0}}-p^{n_{r+1}}}$. Its order is $p^{n_{r+1}}$. Therefore we constructed an action of G on X. By construction we have that the set

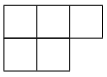
$$\left\{ E_i^{p^{n_i}-1} \mid i = 1, \ldots, s \right\}$$

is K-linearly independent. This set corresponds to the induced action of the socle of G. Hence the action of the socle of G is generically free, and the same is true for the action of G by Proposition 3.2.1. This implies, by Proposition 3.1.15, that $\dim_k(\mathrm{Lie}(G)) \leq n$, as wanted. □

Remark 3.3.12. Notice that actually in the above proof we never used the fact that the H-action was faithful. Moreover we remark that the condition on the existence of such actions is purely combinatorial and it is equivalent to asking, using the notation of the proof, that $\dim_k(\mathrm{Lie}(G)) = \sum_{j=1}^{s} n_j \leq n$. For example, if we take G_1 and G_2 corresponding respectively to

 and 

then

$G =$ 

and the Proposition implies that even if there exist generically free actions of G_i on every variety of dimension 4, there is no action of $G_1 \times_k G_2$ on a variety of dimension 4 which is generically free when restricted to G_i for $i = 1, 2$. On the other hand, there exist such actions on every variety of dimension ≥ 5.

Let us illustrate the above results in the case of the connected part of the p-torsion of abelian varieties.

Example 3.3.13. Let k be algebraically closed and A be an abelian variety defined over k of dimension g, p-rank f and a-number a. If there exists a faithful rational action of $A[p]^0$ on a curve, then by Proposition 3.3.6, $f \leq 1$ and either $A[p]^{0,u}$ is trivial (if $f = 1$) or $V_{\ker(F_{A[p]^{0,u}})} = 0$ (if $f = 0$). In either case, it holds $\mathrm{soc}(A[p]^0) = \ker(F_{A[p]})$. As a consequence one has that $a + f = g$. We then have the following two cases.

- If $f = 1$, then $f = 1 = g$, that is A is an ordinary elliptic curve and faithful rational actions of $A[p]^0 = \mu_p$ on any curve always exist.

- If $f = 0$, then $a = g$ that is A is a superspecial abelian variety. Superspecial abelian varieties are always isomorphic to products of supersingular elliptic curves [Oor75, Theorem 2]. In Example 3.3.7 we saw that there is no faithful rational action of $E[p] \times_k E[p]$ on any curve, for E supersingular.

Therefore, we can conclude that there exists a faithful rational action of $A[p]^0$ on a curve if and only if A is an elliptic curve. More generally, if there exists a faithful rational action of $A[p]^0$ on a variety of dimension n, then $0 \leq g - f \leq a(n - f)$. Indeed, by Proposition 3.3.6, we have $f \leq n$ and $V^{n-f}_{\ker(F_{A[p]^0,u})} = 0$ (if $f = n$ then there is no unipotent part). This means that

$$\ker(F_{A[p]}) \simeq \prod_{i=1}^{a} W^1_{n_i} \times_k \mu_p^f$$

where $n_i \leq n - f$ for every $i \in I$. As a consequence, $g - f = \sum_{i \in I} n_i \leq a(n - f)$.

Notice that if $g \leq n$ we don't get any interesting information and moreover by Remark 3.2.14 there exist always generically free rational actions of $A[p]^0$ on varieties of dimension n. Nevertheless, such faithful rational actions may occur even when $g > n$ (if $n > 1$, as seen in the first part). For example, by Proposition 3.3.10, there exist faithful rational actions of the p-torsion of a superspecial abelian variety of any dimension on any variety of dimension ≥ 2 (but not on curves).

The numerical condition $g - f \leq a(n - f)$ holds true for any $G \simeq G^u \times_k G^d$ infinitesimal commutative trigonalizable k-group scheme with a faithful rational action on a variety of dimension n, with $a = \dim_k(\mathrm{Lie}(\mathrm{soc}(G^u)))$, $f = \dim_k(\mathrm{Lie}(\mathrm{soc}(G^s)))$ and $g = \dim_k(\mathrm{Lie}(G))$.

3.4 Subgroup schemes of $\mathrm{PGL}_{2,k}$ in characteristic 2

The content of this section comes entirely from [GT24]. If the characteristic of a field k is odd any infinitesimal subgroup scheme of $\mathrm{PGL}_{2,k}$ lifts to $\mathrm{SL}_{2,k}$. In this last section, we prove that this is not true in characteristic 2 and we give a complete description, up to isomorphism, of infinitesimal unipotent subgroup schemes of $\mathrm{PGL}_{2,k}$. Also, the infinitesimal trigonalizable case is considered.

In his paper [Bea10], Beauville classified, up to conjugacy, all finite subgroups of $\mathrm{PGL}_2(k)$ of order coprime with the characteristic. Here we are interested in the opposite case, infinitesimal subgroup schemes. It seems that it is quite an accepted fact that any infinitesimal subgroup scheme of $\mathrm{PGL}_{2,k}$ lifts to $\mathrm{GL}_{2,k}$. In particular any unipotent infinitesimal subgroup scheme of $\mathrm{PGL}_{2,k}$ would be a subgroup scheme of $\mathbb{G}_{a,k}$, and so it would be isomorphic to $\alpha_{p^n,k}$ for some $n \geq 0$. We prove that this is not true if the characteristic of the field is 2 (see also Example 3.2.17). The result is instead true if the characteristic is odd and we give a proof of it (see Proposition 3.4.4).

We recall that, for any field k, represents the automorphism group functor of $\mathbb{P}^1_k$. So subgroup schemes of $\mathrm{PGL}_{2,k}$ correspond to faithful actions on $\mathbb{P}^1_k$. Moreover $\mathrm{PGL}_{2,k}(k)$ coincides with the Cremona group in dimension one, i.e. birational self-maps of $\mathbb{P}^1_k$, since any rational self-map of a projective non-singular curve extends to the whole curve. In positive characteristic, the situation is completely different if we consider rational actions of infinitesimal group schemes. Most of the faithful infinitesimal actions of the affine line do not extend to $\mathbb{P}^1_k$. For instance, all the faithful actions of α_p^n, with $n \geq 4$, on $\mathbb{A}^1_k$ do not extend to $\mathbb{P}^1_k$, since $\mathrm{PGL}_{2,k}$ has dimension 3 and the Lie algebra of α_p^n has dimension n. See, for instance, [Bri22, Lemma 3.6] and Proposition 3.3.10.

The main result of this section is the following.

Theorem 3.4.1. *Let k be a field of characteristic 2.*

1. *The infinitesimal unipotent subgroup schemes of $\mathrm{PGL}_{2,k}$ are exactly, up to isomorphism, the subgroup schemes of the semi-direct product $\alpha_{2^n,k} \rtimes \alpha_{2,k}$, with $n \geq 1$, where the action of $\alpha_{2,k}$ on $\alpha_{2^n,k}$ is given by $s \cdot t = t + st^2$.*

2. *If k is perfect, any infinitesimal trigonalizable, not unipotent, subgroup scheme of $\mathrm{PGL}_{2,k}$ is isomorphic to $\mu_{2^l,k}$ or to the semi-direct product of $\mu_{2^l,k}$, for some $l \geq 1$, by one of the two unipotent group schemes*

   (a) *the semi-direct product $\alpha_{2^n,k} \rtimes \alpha_2$, with $n \geq 1$, where the action of $\alpha_{2,k}$ on $\alpha_{2^n,k}$ is given by $s \cdot t = t + st^2$*

   (b) *$\alpha_{2^n,k}$*

   for some non-trivial action of $\mu_{2^l,k}$.

An explicit description of all these group schemes will be given further on. While the above Theorem gives a complete classification of infinitesimal unipotent subgroup schemes of $\mathrm{PGL}_{2,k}$, for trigonalizable group schemes we do not know if, for any non-trivial action of $\mu_{2^l,k}$ on the unipotent group schemes in (a), the associated semi-direct product acts faithfully on $\mathbb{P}^1_k$. At the end of this section, we prove that there exists at least one action of $\mu_{2^l,k}$ on any unipotent group scheme which appears in (a) such that the associated semi-direct product acts faithfully on $\mathbb{P}^1_k$. In the commutative case, we get a complete classification over an algebraically closed field.

Corollary 3.4.2. *Let k be an algebraically closed field of characteristic 2. The list of infinitesimal commutative subgroup schemes of $\mathrm{PGL}_{2,k}$, up to isomorphism, is the following:*

1. *$\alpha_{2^n,k}$, for some $n \geq 0$,*

2. *$\alpha_{2,k} \times \alpha_{2,k}$,*

3. *the 2-torsion of a supersingular elliptic curve,*

4. *μ_{2^n}, for some $n > 0$.*

The Corollary follows from Theorem 3.4.1 by using Lemma 3.4.7. In [Kno95] Knop classified subgroup schemes of $\mathrm{SL}_{2,k}$ up to conjugacy. Of course, it could be possible to deduce Theorem 3.4.1 by computing the quotient of all infinitesimal trigonalizable subgroup schemes of $\mathrm{SL}_{2,k}$. In fact, in our approach, we just need to know infinitesimal unipotent subgroup schemes of $\mathrm{SL}_{2,k}$, which is much easier.

Infinitesimal subgroup schemes of $\mathrm{PGL}_{2,k}$ in characteristic $p > 2$

Let k be a field of characteristic p. If $p > 2$ and G is an infinitesimal subgroup scheme of $\mathrm{PGL}_{2,k}$, since $\mathrm{SL}_{2,k} \to \mathrm{PGL}_{2,k}$ is an étale covering, then G lifts to $\mathrm{SL}_{2,k}$. This result is known and, for instance, it is mentioned in Fakhruddin [Fak20]. We, however, report here the details of the proof, which are not present in the aforementioned paper. We have the following lemma.

Lemma 3.4.3. *Any short exact sequence of algebraic group schemes over a field k*

$$1 \longrightarrow H \xrightarrow{i} G \longrightarrow Q \longrightarrow 1,$$

such that H is étale and Q is infinitesimal, splits and the semi-direct product is in fact direct.

Proof. We firstly observe that G is necessarily a finite group scheme. Let us consider the connected-étale sequence

$$1 \longrightarrow G^0 \longrightarrow G \xrightarrow{\pi} \pi_0(G) \to 1.$$

We remark that G^0 is infinitesimal, since G is finite. Let us consider the morphism $\pi \circ i : H \to \pi_0(G)$. We claim that this is an isomorphism. Indeed, since H and $\pi_0(G)$ are étale, it is enough to prove that $H(\overline{k}) \to \pi_0(G)(\overline{k})$ is an isomorphism, where $\overline{k}$ is an algebraic closure of k. Now we have the factorization

$$H(\overline{k}) \xrightarrow{i(\overline{k})} G(\overline{k}) \xrightarrow{\pi(\overline{k})} \pi_0(G)(\overline{k}).$$

By [Mil17, Corollary 5.48], the morphism $i(\overline{k})$ (resp. $\pi(\overline{k})$) is an isomorphism since $Q(\overline{k})$ (resp. $G^0(\overline{k})$) is trivial. So $\pi \circ i$ is an isomorphism and let f be its inverse. Then $f \circ \pi : G \to H$ is a left inverse of i and therefore the exact sequence in the statement is split and the extension is isomorphic to the natural extension of the direct product. □

Proposition 3.4.4. *If k is a field of characteristic p and p does not divide n then any infinitesimal subgroup scheme of $\mathrm{PGL}_{n,k}$ lifts to $\mathrm{SL}_{n,k}$.*

Proof. We consider the exact sequence

$$1 \to \mu_{n,k} \to \mathrm{SL}_{n,k} \xrightarrow{\pi} \mathrm{PGL}_{n,k} \to 1.$$

Since p does not divide n then $\mu_{n,k}$ is an étale group scheme. Let G be an infinitesimal subgroup scheme of $\mathrm{PGL}_{n,k}$. Then $\pi^{-1}G$ is an extension of G by $\mu_{n,k}$. By the previous Lemma the extension is trivial, so G lifts to $\mathrm{SL}_{n,k}$. □

In particular the above Proposition applies when $n = 2$ and $p > 2$.

Infinitesimal unipotent subgroup schemes of $\mathrm{GL}_{2,k}$

In this subsection, we give an explicit description of all infinitesimal unipotent subgroup schemes of $\mathrm{GL}_{2,k}$, where k is a field of positive characteristic p. The following result will be used in the proof of Theorem 3.4.1.

Proposition 3.4.5. *Any infinitesimal unipotent subgroup scheme of $\mathrm{GL}_{2,k}$ is one of the following subgroup schemes of $\mathrm{SL}_{2,k}$*

$$H_{s_1,s_2,n} = \{\left(\begin{smallmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{smallmatrix}\right) \in \ker F^n_{\mathrm{SL}_{2,k}} | s_i(x_{ii}-1) + s_j(x_{ij}) = 0, x_{22} = 2 - x_{11} \text{ for } i \neq j\},$$

for some $[s_1 : s_2] \in \mathbb{P}^1(k)$ and $n \geq 1$.

Proof. Any infinitesimal unipotent subgroup scheme of $\mathrm{GL}_{2,k}$ is isomorphic to $\alpha_{p^n,k}$, for some n, since by [DG70, IV.§2, Proposition 2.5(iv)], up to conjugation, it is contained in the subgroup of upper triangular unipotent matrices, which is isomorphic to $\mathbb{G}_{a,k}$. Moreover any unipotent subgroup scheme H of $\mathrm{GL}_{2,k}$ is contained in $\mathrm{SL}_{2,k}$ since, over a field, any homomorphism from a unipotent group scheme to a diagonalizable group scheme is trivial, so the restriction of the determinant to H is trivial. We now observe that

$$\mathcal{H}om_{gr}(\alpha_{p^n,k}, \mathrm{SL}_{2,k}) \subseteq \mathrm{SL}_{2,k}(k[T]/(T^{p^n}))$$

and it consists of matrices $A(T)$ such that

$$A(S+T) = A(S)A(T)$$

in $\mathrm{SL}_{2,k}(k[S,T]/(S^{p^n}, T^{p^n})$. Since $A(0) = \mathrm{id}$ we have

$$A(T) = \sum_{i=0}^{p^n-1} A_i T^i$$

with $A_i \in M_2(k)$ for any $0 \leq i \leq p^n - 1$ and $A_0 = \mathrm{id}$. Now

$$A(S+T) = \sum_{i=0}^{p^n-1} \sum_{j=0}^{i} \binom{i}{j} A_i S^j T^{i-j}$$

and

$$A(S)A(T) = \sum_{i,j=0}^{p^n-1} A_i A_j S^i T^j.$$

Therefore for any $0 \leq i, j < p^n$ we have

$$\binom{i+j}{j} A_{i+j} = A_i A_j$$

where we set $A_k = 0$ if $k \geq p^n$. Then

$$A_i^p = \binom{2i}{i} \cdots \binom{pi}{i} A_{pi} = \frac{(pi)!}{(i!)^p} A_{pi}$$

for any $0 \leq i \leq p^n - 1$. Now

$$v_p\Big(\frac{(pi)!}{(i!)^p}\Big) = i - (p-1)v_p(i!) > 0,$$

so

$$A_i^p = 0.$$

Moreover A_i commutes with A_j for any $0 \leq i, j \leq p^n - 1$. It is known that if two non-zero nilpotent matrices of size 2 commute then one is a multiple of the other. Therefore there exists a nilpotent matrix $B \in M_2(k)$ and $f(T) \in k[T]/(T^{p^n})$ such that $A(T) = \mathrm{id} + Tf(T)B$. Now it is easy to verify that $f(T)$ is additive. Then the matrix $A(T)$ belongs to $H_{s_1,s_2,n}(k[T]/(T^{p^n}))$, where $(s_1, s_2) \in \ker B \setminus \{(0,0)\}$. So any infinitesimal unipotent subgroup scheme of $\mathrm{GL}_{2,k}$ is contained in $H_{s_1,s_2,n}$ for some $[s_1 : s_2] \in \mathbb{P}^1(k)$. On the other hand, for any $[s_1 : s_2] \in \mathbb{P}^1(k)$ the matrix

$$A(T) = \mathrm{id} + T \begin{pmatrix} s_1 s_2 & -s_1^2 \\ s_2^2 & -s_1 s_2 \end{pmatrix}$$

gives an isomorphism between $\alpha_{p^n,k}$ and $H_{s_1,s_2,n}$.

□

Some non-commutative infinitesimal unipotent group schemes

In this subsection we explicitly describe the group schemes appearing in Theorem 3.4.1.

Definition 3.4.6. Let k be a field of characteristic p and consider the action of $\alpha_{p,k}$, by group scheme automorphisms, on $\mathbb{G}_{a,k}$ given by $s \cdot t = t + st^p$. We define the associated semi-direct product $\mathcal{E} = \mathbb{G}_{a,k} \rtimes \alpha_{p,k}$.

1. For any $n \geq 0$ we define the subgroup scheme $\mathcal{D}_n$ of $\mathcal{E}$ as the induced semi-direct product $\alpha_{p^n} \rtimes \alpha_{p,k}$.

2. For any $a \in k$ and $n \geq 1$, we define $\mathcal{H}_{a,n}$ as the kernel of the morphism

$$(-aF^{n-1}, i) : \mathcal{D}_n \to \mathbb{G}_{a,k}$$

where i is the inclusion $i : \alpha_{p,k} \to \mathbb{G}_{a,k}$, that is $\mathcal{H}_{a,n} = \Big\{(t,s) \in \mathcal{D}_n \mid s = at^{p^{n-1}}\Big\}$.

Explicitly we have that $\mathcal{D}_n$ is isomorphic to $\mathrm{Spec}(k[S,T]/(S^p, T^{p^n})$ where the comultiplication is given by

$$S \mapsto S \otimes 1 + 1 \otimes S$$

and

$$T \mapsto T \otimes 1 + 1 \otimes T + S \otimes T^p.$$

We observe that, for $p = 2$, this is the group that appears in the statement of Theorem 3.4.1. The previous group scheme is equally isomorphic to $\mathrm{Spec}\, k[S,T]/(S^p, T^{p^n})$, where the comultiplication is given by

$$S \mapsto S \otimes 1 + 1 \otimes S$$

and

$$T \mapsto T \otimes 1 + 1 \otimes T + T^p \otimes S.$$

The two group schemes are isomorphic via $S \mapsto S, T \mapsto T + ST^p$. We will need this second presentation in the proof of Theorem 3.4.1.

Moreover $\mathcal{H}_{a,n}$ is isomorphic to $\operatorname{Spec} k[T]/(T^{p^n})$ where the comultiplication is given by

$$T \mapsto T \otimes 1 + 1 \otimes T + aT^{p^{n-1}} \otimes T^p.$$

Notice that for $n > 2$ and $a \neq 0$, these are all examples of infinitesimal unipotent group schemes that are not commutative. We collect some easy results that will be freely used further on.

Lemma 3.4.7. *Let k be a field of characteristic p.*

1. *$\mathcal{D}_0$ is isomorphic to $\alpha_{p,k}$ and $\mathcal{D}_1$ is isomorphic to $\alpha_{p,k} \times \alpha_{p,k}$.*
2. *For any $n \geq 2$, $\mathcal{H}_{0,1}$ is the center of $\mathcal{D}_n$ and $\mathcal{D}_n/\mathcal{H}_{0,1}$ is isomorphic to $\alpha_{p^{n-1},k} \times \alpha_{p,k}$.*
3. *$\mathcal{H}_{a,n}$ is commutative if and only if $n \leq 2$ or $a = 0$.*
4. *$\mathcal{H}_{0,n}$ is isomorphic to $\alpha_{p^n,k}$ and $\mathcal{H}_{a,1}$ is isomorphic to $\alpha_{p,k}$.*
5. *If $a \neq 0$, $\mathcal{H}_{a,2}$ is isomorphic to $\alpha_{p^2,k}$ if $p > 2$, and to a form of the 2-torsion of a supersingular elliptic curve if $p = 2$.*
6. *If $n \geq l \geq 0$, $\mathcal{D}_l$ is a closed subgroup scheme of $\mathcal{D}_n$, and if $l \geq 1$, $\mathcal{D}_l = \ker F^l_{\mathcal{D}_n}$.*

Proof. All the proofs, except (5), are straightforward. If $char(k) > 2$, $\mathcal{H}_{a,2}$ is isomorphic to $\alpha_{p^2,k}$ via the isomorphism $T \mapsto T - a\frac{T^{2p}}{2}$. If $char(k) = 2$ and k algebraically closed, $\mathcal{H}_{a,2}$ is isomorphic to $\mathcal{H}_{1,2}$, via $T \mapsto cT$ where c is a cubic root of a (see also Lemma 3.4.11 for more details). And $\mathcal{H}_{1,2}$ is isomorphic to $\ker(F - V : W_{2,k} \to W_{2,k})$, where $W_{2,k}$ is the group scheme of Witt vectors of length 2 and V is the Verschiebung. This group scheme is known to be isomorphic to the 2-torsion of a supersingular elliptic curve (we also give a proof of this in Chapter 2, see Corollary 2.3.10). □

Remark 3.4.8. If $n \geq 3$ and $a \neq 0$, $\mathcal{H}_{a,n}$ is a subgroup scheme of the non-abelian extension of $\mathbb{G}_a$ by $\mathbb{G}_a$ given by the cocycle $aT^pT'^{p^{n-1}}$ (see [DG70, II, §3, 4.6]).

Lemma 3.4.9. *Let $n \geq 0$. Any closed subgroup scheme of $\mathcal{D}_n$ is equal to $\mathcal{D}_l$, with $0 \leq l \leq n$, or to $\mathcal{H}_{a,m}$, for some $a \in k$ and $1 \leq m \leq n$.*

Proof. The result is clear for $n \leq 1$. So we suppose $n \geq 2$. In particular, $\mathcal{D}_n$ is not commutative. Let H be a closed subgroup scheme of $\mathcal{D}_n$. If $H \subseteq \ker F^l_{\mathcal{D}_n}$, for some $0 \leq l < n$, then H is a closed subgroup scheme of $\mathcal{D}_l$. Up to taking a minimal $0 \leq l \leq n$ such that $F^l_H = 0$, we can suppose that $F^{n-1}_H \neq 0$. In particular, if H is a proper subgroup scheme of $\mathcal{D}_n$, then H has order p^n (otherwise iterating $n-1$ times the Frobenius, which has a kernel of order at least p, we will get the trivial morphism). Suppose that H

does not contain the center $\mathcal{H}_{0,1}$ of $\mathcal{D}_n$. Then, by dimension reasons, the natural map $H \times \mathcal{H}_{0,1} \to \mathcal{D}_n$ is an isomorphism. Hence $H \simeq \mathcal{D}_n/\mathcal{H}_{0,1} \simeq \alpha_{p^{n-1},k} \times \alpha_{p,k}$, which would imply that $\mathcal{D}_n$ is commutative. Therefore H contains the center of $\mathcal{D}_n$. As a consequence, $H/\mathcal{H}_{0,1}$ is a closed subgroup scheme of $\mathcal{D}_n/\mathcal{H}_{0,1} \simeq \alpha_{p^{n-1},k} \times \alpha_{p,k}$. In particular, $H/\mathcal{H}_{0,1}$ is a normal subgroup scheme of $\mathcal{D}_n/\mathcal{H}_{0,1}$, which implies that H is a normal subgroup scheme of $\mathcal{D}_n$. So H is obtained as the kernel of a morphism from $\mathcal{D}_n$ to α_p. Any such a morphism is given by an element

$$P(S,T) = \sum_{0\leq i<p, 0\leq j<p^n} a_{ij} S^i T^j \in k[S,T]/(S^p, T^{p^n})$$

such that $P(S,T)^p = 0$ and

$$\sum_{\substack{0\leq i<p\\ 0\leq j<p^n}} a_{ij}(S\otimes 1+1\otimes S)^i(T\otimes 1+1\otimes T+T^p\otimes S)^j = \sum_{\substack{0\leq i<p\\ 0\leq j<p^n}} a_{ij}(S^iT^j\otimes 1+1\otimes S^iT^j) \quad (3.2)$$

in $k[S,T]/(S^p,T^{p^n}) \otimes k[S,T]/(S^p,T^{p^n})$. We can suppose $a_{00} = 0$. If we reduce modulo $(T)\otimes(1)$ we get

$$\sum_{\substack{0\leq i<p\\ 0\leq j<p^n}} a_{ij}(S\otimes 1+1\otimes S)^i(1\otimes T^j) = \sum_{\substack{0\leq i<p\\ 0<j<p^n}} a_{ij}(1\otimes S^iT^j) + \sum_{0<i<p} a_{i0}(1\otimes S^i + S^i\otimes 1).$$

in $k[S]/(S^p)\otimes k[S,T]/(S^p,T^{p^n})$. Therefore $a_{ij} = 0$ if $1 < i < p$ or $i = 1$ and $j > 0$. So

$$P(S,T) = a_{1,0}S + Q(T).$$

If we reduce (3.2) modulo $(1)\otimes(S)$ we find that $Q(T)$ is additive. Since $P(S,T)^p = 0$ we get that $P(S,T) = a_{10}S + a_{0p^{n-1}}T^{p^{n-1}}$. Moreover, $a_{10} \neq 0$ since we supposed that $F_H^{n-1} \neq 0$. So we have that H is isomorphic to $\mathcal{H}_{a,n}$, with $a = \frac{a_{0p^{n-1}}}{a_{10}}$. □

Lemma 3.4.10. *Let G be an infinitesimal unipotent group scheme with one-dimensional Lie algebra over a field of characteristic p. An action, as a group scheme automorphism, of an infinitesimal group scheme H of multiplicative type on G is faithful if and only if the induced action on* $\ker F_G$ *is faithful. And, if this happens, H has one-dimensional Lie algebra.*

Proof. The 'if' part is obvious. We prove the 'only if' part. We can suppose that H is of height 1 since the kernel of any action of an infinitesimal group scheme has a non-trivial Frobenius kernel. We also remark that $\dim_k(\mathrm{Lie}(H)) = \dim_k(\mathrm{Lie}(\ker F_H))$. Therefore, by [DG70, III, §6, Proposition 7.1], H is a subgroup scheme of $\mathcal{A}ut_1(G) = \ker(\mathcal{A}ut(G) \to \mathcal{A}ut(G/\ker F_G))$. Moreover, $\ker F_G \simeq \alpha_p$ is contained in the center since a unipotent group scheme has a non-trivial center, and, since G is infinitesimal unipotent, the intersection with the kernel of the Frobenius is non-zero. Therefore the induced action of $G/\ker F_G$ on $\ker F_G$ is trivial, then, by [DG70, III, §6, Proposition 7.4], we have an exact sequence

$$0 \to \mathcal{H}om_{gr}(G/\ker F_G, \alpha_p) \longrightarrow \mathcal{A}ut_1(G) \longrightarrow \mathcal{A}ut_{gr}(\ker F_G) \simeq \mathbb{G}_{m,k}.$$

Remark that $\mathcal{H}om_{gr}(\alpha_p, \alpha_p) \simeq \mathbb{G}_{a,k}$, so, by dévissage, we get that $\mathcal{H}om_{gr}(G/\ker F_G, \alpha_p)$ is a unipotent group scheme. Since H is of multiplicative type, its intersection with $\mathcal{H}om_{gr}(G/\ker F_G, \alpha_p)$ is trivial. As a consequence, H embeds in $\mathcal{A}ut_{gr}(\ker F_G) \simeq \mathbb{G}_{m,k}$, that is H acts faithfully on $\ker F_G$. Moreover, since we showed that H is a k-subgroup scheme of height 1 of $\mathbb{G}_{m,k}$, then H is isomorphic to $\mu_{p,k}$ and so its Lie algebra is one-dimensional.

□

Lemma 3.4.11. *Let k be a field of characteristic p and let $n > 2$ or ($n = 2$ and $p = 2$).*

1. *Any action of $\mu_{p,k}$ on $\mathcal{H}_{0,n} \simeq \alpha_{p^n,k}$, as group scheme automorphism, is conjugate to $v \cdot t = v^i t$, for some $0 \leq i \leq p-1$. Therefore, for any non-trivial action of $\mu_{p,k}$ on $\alpha_{p^n,k}$, all semi-direct products $\alpha_{p^n,k} \rtimes \mu_p$ are isomorphic.*
2. *If $a, b \in k \setminus \{0\}$, then $\mathcal{H}_{a,n}$ is isomorphic to $\mathcal{H}_{b,n}$ if and only if b/a is a (p^n+p-1)-th power.*
3. *There are no non-trivial actions, as group scheme automorphism, of infinitesimal group schemes of multiplicative type on $\mathcal{H}_{a,n}$, for any $a \in k \setminus \{0\}$.*

Proof.

1. It is easy to see that the homomorphism $\mathcal{A}ut_{gr}(\mathbb{G}_a) \to \mathcal{A}ut_{gr}(\alpha_{p^n})$ admits a section. Therefore any action of $\mu_{p,k}$ on $\alpha_{p^n,k}$ extends to an action on $\mathbb{G}_{a,k}$. Now, by [DG70, III, §6, Corollaire 7.9], we have that any action of $\mu_{p,k}$ on $\mathbb{G}_{a,k}$ is given by
$$v \cdot x = v^i x + (v^i - 1) \sum_{l=1}^{s} a_l x^{p^l}$$
for some $s \geq 1$, $0 \leq i \leq p-1$ and $a_i \in k$ for any $1 \leq l \leq s$. Therefore any action of $\mu_{p,k}$ on $\alpha_{p^n,k}$ is given by
$$v \cdot x = v^i x + (v^i - 1) \sum_{l=1}^{p^n-1} a_l x^{p^l}$$
for some $a_i \in k$ for any $1 \leq l \leq p^{n-1} - 1$ and $0 \leq i \leq p-1$. But this action is conjugated to the action $v \cdot x = v^i x$ via the automorphism $x \mapsto x + \sum_{l=1}^{p^n-1} a_l x^{p^l}$. If the action is non-trivial, then $i > 0$. Moreover, $v \mapsto v^i$ is an automorphism of $\mu_{p,k}$, therefore all the associated semi-direct products are isomorphic.

2, 3. We recall that the Hopf algebra of $\mathcal{H}_{a,n}$ is isomorphic to $k[T]/(T^{p^n})$, where the comultiplication is given by $T \otimes 1 + 1 \otimes T + aT^{p^{n-1}} \otimes T^p$. We now consider an element of $\mathcal{I}som(\mathcal{H}_{a,n}, \mathcal{H}_{b,n})(R)$, with R a k-algebra. An isomorphism from $\mathcal{H}_{a,n,R}$ to $\mathcal{H}_{b,n,R}$ is given by an element $P(T) = \sum_{i=1}^{p^n-1} a_i T^i \in R[T]/(T^{p^n})$ such that $a_1 \in R$ is invertible and
$$\sum_{i=1}^{p^n-1} a_i (T^i \otimes 1 + 1 \otimes T^i) + a \Big(\sum_{i=1}^{p-1} a_i^{p^{n-1}} T^{ip^{n-1}}\Big) \otimes \Big(\sum_{i=1}^{p^{n-1}-1} a_i^p T^{ip}\Big) =$$

$$\sum_{i=1}^{p^n-1} a_i(T\otimes 1 + 1\otimes T + bT^{p^{n-1}}\otimes T^p)^i.$$

Since it induces an isomorphism on the kernels of the p^{n-1}-th power of the Frobenius, which are isomorphic to $\alpha_{p^{n-1},R}$, we get that $a_i = 0$ if $1 < i < p^{n-1}$ and i is not a power of p. Moreover, $a_i = 0$ if $i > p^{n-1}$ and i is not divisible by p (one can see it by differentiating both sides). So we get

$$\sum_{r=p^{n-2}+1}^{p^{n-1}-1} a_{pr}(T^{pr}\otimes 1 + 1\otimes T^{pr}) + aa_1^{p^{n-1}}T^{p^{n-1}}\otimes(\sum_{r=0}^{n-2} a_{p^r}^p T^{p^{r+1}}) =$$

$$\sum_{r=p^{n-2}+1}^{p^{n-1}-1} a_{pr}(T^p\otimes 1 + 1\otimes T^p)^r + a_1 bT^{p^{n-1}}\otimes T^p.$$

If $n > 2$ and $a \neq 0$, comparing the coefficients of $T^p\otimes T^{p^{n-1}}$, we get $a_{p^{n-1}+p} = 0$ and, comparing the coefficients of $T^{p^{n-1}}\otimes T^p$, we get $aa_1^{p^{n-1}+p} = a_1 b$, which means that a_1 is a $(p^{n-1}+p-1)$-th power of b/a. If $n = 2$ and $p = 2$ the above equality reduces to

$$aa_1^{2+2}T^p\otimes T^p = a_1 bT^p\otimes T^p,$$

so a_1 is a cubic root of b/a. If $R = k$ this proves that $\mathcal{H}_{a,n}$ is isomorphic to $\mathcal{H}_{b,n}$ if and only if b/a is a (p^n+p-1)-th power. But this also proves that, if $a \neq 0$, the image of the map $\mathcal{A}ut(\mathcal{H}_{a,n}) \to \mathcal{A}ut(\ker F_{\mathcal{H}_{a,n}})$ is contained in $\mu_{p^{n-1}+p-1,k}$. Let H be an infinitesimal group scheme of multiplicative acting on $\mathcal{H}_{a,n}$ via $\rho : H \to \mathcal{A}ut(\mathcal{H}_{a,n})$. Then the image of $\rho(H)$ via $\mathcal{A}ut(\mathcal{H}_{a,n}) \to \mathcal{A}ut(\ker F_{\mathcal{H}_{a,n}})$ lies in $\mu_{p^{n-1}+p-1,k}$, that is it is trivial, since $\mu_{p^{n-1}+p-1,k}$ is étale and $\rho(H)$ infinitesimal. As a consequence, the induced faithful action of $\rho(H)$ on $\ker(F_{\mathcal{H}_{a,n}})$ is trivial and thus, by Lemma 3.4.10, also the faithful action of $\rho(H)$ on $\mathcal{H}_{a,n}$ (and thus that of H) is trivial. Therefore, any infinitesimal group scheme of multiplicative type acts trivially on $\mathcal{H}_{a,n}$ if $a \neq 0$. On the other hand, if $a_1 \in k$ is such that $a_1^{p^n+p-1} = b/a$ then the polynomial $P(T) = a_1 T$ gives an isomorphism for any $n \geq 1$ and any prime p.

□

Proof of Theorem 3.4.1

We start with a Lemma.

Lemma 3.4.12. *Let k be a field of characteristic 2 and G be a unipotent subgroup scheme of* $\mathrm{PGL}_{2,k}$. *Then*

1. $\ker F_G$ *is isomorphic to* $\alpha_{2,k}$ *or to* $\alpha_{2,k}\times\alpha_{2,k}$;
2. $\mathrm{Im}\, F_G$ *is isomorphic to* $\alpha_{2^n,k}$, *for some* n.

Proof.

1. We observe that in characteristic 2 we have the following exact sequence of restricted p-algebras
$$0 \to \mathrm{Lie}(\mathbb{G}_a^2) \to \mathfrak{pgl}_2 \to \mathrm{Lie}(\mathbb{G}_m) \to 0.$$
Therefore $\mathrm{Lie}(\ker F_G)$ is necessarily contained in $\mathrm{Lie}(\mathbb{G}_a^2)$, which implies that $\ker F_G$ is a subgroup scheme of $\mathbb{G}_a^2$. So we are done.

2. Let $\widetilde{G} := \pi^{-1}G$, where $\pi : \mathrm{SL}_{2,k} \to \mathrm{PGL}_{2,k}$ is the projection. Then we have an exact sequence
$$1 \to \mu_{2,k} \to \widetilde{G} \to G \to 1$$
which yields the following commutative diagram
$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_{2,k} & \longrightarrow & \widetilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle F_{\mu_{2,k}}} & & \downarrow{\scriptstyle F_{\widetilde{G}}} & & \downarrow{\scriptstyle F_G} & & \\ 1 & \longrightarrow & \mu_{2,k} & \longrightarrow & \widetilde{G}^{(p)} & \longrightarrow & G^{(p)} & \longrightarrow & 1 \end{array}$$
where the vertical maps are the relative Frobenius. Since the Frobenius is trivial on $\mu_{2,k}$, we get that F_G factorizes as
$$G \xrightarrow{\alpha} \widetilde{G}^{(p)} \to G^{(p)}.$$
Since G is unipotent then $\alpha(G)$ is a unipotent subgroup of $\widetilde{G}^{(p)} \subseteq \mathrm{SL}_{2,k}$. Therefore $\alpha(G)$ is isomorphic to $\alpha_{2^n,k}$, for some n. So the statement follows.

□

We now continue with the proof of Theorem 3.4.1. Let G be a unipotent subgroup scheme of $\mathrm{PGL}_{2,k}$. Let us consider $\widetilde{G} := \pi^{-1}G \subseteq \mathrm{SL}_{2,k}$. For any $n \geq 1$, we apply the Snake Lemma to this commutative diagram with exact rows
$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_{2,k} & \longrightarrow & \widetilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle F^n_{\mu_{2,k}}} & & \downarrow{\scriptstyle F^n_{\widetilde{G}}} & & \downarrow{\scriptstyle F^n_G} & & \\ 1 & \longrightarrow & \mu_{2,k} & \longrightarrow & \widetilde{G}^{(p^n)} & \longrightarrow & G^{(p^n)} & \longrightarrow & 1 \end{array}$$
and we get an exact sequence
$$1 \to \mu_{2,k} \to \ker F^n_{\widetilde{G}} \to \ker F^n_G \to 1,$$
since there are no non-trivial morphisms from a unipotent group scheme to a diagonalizable group scheme. We also observe that $\ker F^n_{\widetilde{G}} = \pi^{-1}(\ker F^n_G)$.

Let us firstly suppose that $\dim_k(\mathrm{Lie}\, G = 2)$. Then $\ker F_G$ has order 2^2, so $\ker F_{\widetilde{G}}$ has order 2^3 and therefore it coincides with $\ker F_{\mathrm{SL}_{2,k}}$. Now, $\mathrm{Im}\, F_G = \mathrm{Im}\, F_{\widetilde{G}}$, and, by

Lemma 3.4.12, they are both isomorphic to α_{2^n} for some $n \geq 0$. So we have the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \ker F_{\mathrm{SL}_{2,k}} & \longrightarrow & \widetilde{G} & \longrightarrow & \alpha_{p^n} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \ker F_{\mathrm{SL}_{2,k}} & \longrightarrow & \ker F^{n+1}_{\mathrm{SL}_{2,k}} & \xrightarrow{F_{\mathrm{SL}_{2,k}}} & \ker F^{n}_{\mathrm{SL}_{2,k}} & \longrightarrow & 0. \end{array}$$

The diagram is a pull-back since it is a morphism of extensions. By Lemma 3.4.5, any unipotent subgroup of $\ker F^n_{\mathrm{SL}_{2,k}}$ is

$$H_{s_1,s_2,n} = \{\left(\begin{smallmatrix} x_{11} & x_{12} \\ x_{21} & x_{11} \end{smallmatrix}\right) \in \ker F^n_{\mathrm{SL}_{2,k}} | s_i(x_{11}-1) + s_j(x_{ij}) = 0, \text{ for } (i,j) = (1,2),(2,1)\}$$

for some $[s_1 : s_2] \in \mathbb{P}^1(k)$. We are going to prove that, for any $[s_1 : s_2] \in \mathbb{P}^1(k)$, $G = F^{-1}_{\mathrm{SL}_{2,k}}(H_{s_1,s_2,n})/\mu_{2,k}$ is isomorphic to $\mathcal{D}_n$. This would also prove the Theorem in the case $\dim_k(\mathrm{Lie}(G)) = 1$, since $\widetilde{G}$ is contained in the pull-back $F^{-1}_{\mathrm{SL}_{2,k}}(H_{s_1,s_2,n})$, therefore G is a subgroup scheme of $F^{-1}_{\mathrm{SL}_{2,k}}(H_{s_1,s_2,n})/\mu_{2,k} \simeq \mathcal{D}_n$. We firstly remark that $F^{-1}_{\mathrm{SL}_{2,k}}(H_{s_1,s_1,n})/\mu_{2,k}$ has order p^{n+2}. The Hopf algebra of $F^{-1}_{\mathrm{SL}_{2,k}}(H_{s_1,s_2,n})$ is $k[X_{ij}]_{1\leq i,j\leq 2}$ quotiented by the ideal

$$\left((X_{ii}-1)^{2^{n+1}}, X_{ij}^{2^{n+1}}, (X_{ii}-X_{jj})^2, X_{ii}X_{jj} - X_{ij}X_{ji} - 1, s_i(X_{ii}^2-1) + s_j(X_{ij}^2))\right)_{i\neq j}$$

and the comultiplication is induced by

$$X_{ij} \mapsto X_{i1}X_{1j} + X_{i2}X_{2j}$$

for any $1 \leq i,j \leq 2$. Now we compute the invariant ring by the natural action of $\mu_{2,k}$. We let $Y_{ijkl} = X_{ij}X_{kl}$. Consider the subalgebra A of $k[F^{-1}_{\mathrm{SL}_{2,k}}(H_{s_1,s_2})]$ generated by Y_{1112} and Y_{2122}. We suppose $s_1 \neq 0$. If not, $s_2 \neq 0$ and a similar argument works. Looking at the comultiplication we have

$$\begin{aligned} Y_{1112} \mapsto & (X_{11}\otimes X_{11} + X_{12}\otimes X_{21})(X_{11}\otimes X_{12} + X_{12}\otimes X_{22}) = \\ & Y_{1111}\otimes Y_{1112} + Y_{1112}\otimes Y_{1122} + Y_{1112}\otimes Y_{1221} + Y_{1212}\otimes Y_{2122} = \\ & Y_{1111}\otimes Y_{1112} + Y_{1112}\otimes (Y_{1122}+Y_{1221}) + Y_{1112}^2\otimes s_1 Y_{2122} = \\ & Y_{1112}\otimes 1 + 1\otimes Y_{1112} + Y_{1112}^2\otimes (s_1Y_{2122} + s_2Y_{1112}) \end{aligned}$$

and

$$\begin{aligned} Y_{2122} \mapsto & (X_{21}\otimes X_{11} + X_{22}\otimes X_{21})(X_{21}\otimes X_{12} + X_{22}\otimes X_{22}) = \\ & Y_{2121}\otimes Y_{1112} + Y_{2122}\otimes Y_{1122} + Y_{2122}\otimes Y_{1221} + Y_{2222}\otimes Y_{2122} = \\ & Y_{2121}\otimes Y_{1112} + Y_{2122}\otimes (Y_{1122}+Y_{1221}) + Y_{2222}\otimes Y_{2122} = \\ & Y_{2212}\otimes 1 + 1\otimes Y_{2212} + Y_{1112}^2\otimes (s_2Y_{2122} + \frac{s_2^2}{s_1}Y_{1112}) \end{aligned}$$

where we used that $Y_{1122} + Y_{1221} = 1, s_1 Y_{1112}^2 = Y_{1212}$, $s_1 Y_{2121} = s_2^2 Y_{1112}^2$ and $Y_{2222} = Y_{1111} = 1 + s_2 Y_{1112}^2$, which are easy to verify. The antipode is the identity, so A is a Hopf algebra contained in $k[(F_{SL_2}^{-1}(H_{s_1,s_2})]^{\mu_{2,k}}$. We also stress that

$$(s_1 Y_{2122} + s_2 Y_{1112}) \mapsto (s_1 Y_{2212} + s_2 Y_{1112}) \otimes 1 + 1 \otimes (s_1 Y_{2212} + s_2 Y_{1112})$$

and $s_1 Y_{2122} + s_2 Y_{1112}$ is not zero. Indeed for example the element $\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$, with $a^2 = 0$ and $a \neq 0$, belongs to $F_{SL_2}^{-1}(H_{s_1,s_2})$. This means that $s_1 Y_{2122} + s_2 Y_{1112}$ generates a Hopf algebra B isomorphic to $\alpha_{2,k}$. Therefore there is an epimorphism $H = \operatorname{Spec} A \to \operatorname{Spec} B$. The kernel of this map is the spectrum of the algebra generated by the class of Y_{1112} modulo $s_1 Y_{2122} + s_2 Y_{1112}$. This group scheme is isomorphic to $\alpha_{2^{n+1}}$, since $Y_{1112}^{2^n} = X_{11}^{2^n} Y_{12}^{2^n} \neq 0$. Here we use that $s_1 \neq 0$. If $s_1 = 0$, we would have $Y_{2212}^{2^n} \neq 0$. So H has order 2^{n+2}. Since it has the same order as $F_{SL_2}^{-1}(H_{s_1,s_2,n})$, the natural map $F_{SL_2}^{-1}(H_{s_1,s_2}, n) \to H$ is an isomorphism. Moreover H is isomorphic to $\mathcal{D}_n$ via the isomorphism

$$S \mapsto s_1 Y_{2122} + s_2 Y_{1112}$$

and

$$T \mapsto Y_{2122}.$$

Finally let us suppose that k is a perfect field. Then any infinitesimal trigonalizable group scheme T is a semi-direct product $U \rtimes D$, where U is unipotent and D is diagonalizable (see [DG70, IV, §2, Proposition 3.5]). If T is infinitesimal, not unipotent, and a closed subgroup scheme of $\mathrm{PGL}_{2,k}$, that is T acts faithfully on $\mathbb{P}_k^1$, then also D acts faithfully on $\mathbb{P}_k^1$. Faithful actions of diagonalizable group schemes are generically free (see Corollary 3.3.2) and thus, by Proposition 3.1.15, $\dim_k(\mathrm{Lie}(D)) \leq 1$ that is $D \simeq \mu_{2^l,k}$, for some $l \geq 1$. Moreover, by Corollary 3.3.4, D is a normal subgroup scheme of T if and only if U is trivial; if it is not the case, then the action of D on U must be non-trivial. Therefore, by the first part of the Theorem and by Lemma 3.4.11(3), U is isomorphic to $\mathcal{D}_n$ or to $\alpha_{2^n,k}$, for some $n \geq 1$.

Actions of trigonalizable group schemes on $\mathbb{P}_k^1$

In Theorem 3.4.1 we proved that if k is a perfect field of characteristic 2, any trigonalizable, not unipotent nor diagonalizable, infinitesimal subgroup scheme of $\mathrm{PGL}_{2,k}$ is a semi-direct product of $\mu_{2^l,k}$ by $\mathcal{D}_n$ or α_{2^n}, for some $n, l \geq 0$. In this section, we say something more about which semi-direct products can appear.

Proposition 3.4.13. *Let k be a field of characteristic 2 and recall that $\mathcal{E} = \mathbb{G}_{a,k} \rtimes \alpha_{2,k}$ where the action is given by $s \cdot t = t + st^2$. There exists a non-trivial action, as a group scheme automorphism, of $\mathbb{G}_{m,k}$ on $\mathcal{E}$ such that $\mathcal{E} \rtimes \mathbb{G}_{m,k}$ acts faithfully on $\mathbb{P}_k^1$. Moreover, we can choose the action of $\mathbb{G}_{m,k}$ such that, for any $n \geq 0$, it preserves $\mathcal{D}_n$ and $\mathcal{H}_{0,n}$. We then obtain, by restriction, faithful actions of the induced semi-direct products $\mathcal{D}_n \rtimes \mu_{2^l,k}$ and $\mathcal{H}_{0,n} \rtimes \mu_{2^l,k}$ on $\mathbb{P}_k^1$, for any $l \geq 1$.*

Proof. Let us consider the action of $\mathbb{G}_{m,k} = \operatorname{Spec} k[V, V^{-1}]$ on $\mathcal{E}$ given by $v \cdot (s,t) = (v^{-1}s, vt)$. Then we define the action of $\mathcal{E} \rtimes \mathbb{G}_{m,k}$ on $\mathbb{A}^1_k = \operatorname{Spec} k[X]$ given by the coaction

$$X \longmapsto VX + V^2SX^2 + T.$$

And we get

$$\frac{1}{X} \longmapsto \frac{1}{T+VX}\Big(1 + \frac{V^2SX^2}{T+VX}\Big) = \\ S + \frac{1}{T+VX} + \frac{T^2S}{(T+VX)^2} \in k[X, T, V^{\pm 1}, (T+VX)^{-1}][S]/(S^2).$$

Therefore, by gluing, we get a faithful action of $\mathcal{E} \rtimes \mathbb{G}_{m,k}$ on $\mathbb{P}^1_k$.

□

Remark 3.4.14.

1. The group scheme $\ker F_{\mathrm{PGL}_{2,k}}$ is isomorphic to the semi-direct product $\alpha^2_{2,k} \rtimes \mu_{2,k}$, where the action is given by $v \cdot (s,t) = (vs, vt)$. Indeed it coincides with the kernel of the Frobenius of the group scheme constructed in the Proposition.

2. We remark that taking $V = 1$ in the proof of the Proposition, we get an explicit faithful action on $\mathbb{P}^1_k$ of any infinitesimal unipotent subgroup scheme of $\mathrm{PGL}_{2,k}$, since, as proved in the Theorem, they are all subgroup schemes of $\mathcal{E}$.

We finally mention the following Lemma.

Lemma 3.4.15. *Let k be a perfect field of characteristic 2. Up to isomorphism, there is a unique infinitesimal trigonalizable subgroup scheme of $\mathrm{PGL}_{2,k}$ extension of μ_2 by α_{2^n}, for any $n > 0$.*

Proof. This follows from Theorem 3.4.1 and Lemma 3.4.11(1). □

Appendices

Appendix A

Smash products and Azumaya algebras

This appendix focuses on the smash product algebra. As seen in Chapter 1, an example of smash product is given by the algebra of Ore polynomials. Along with linearised polynomials, Ore polynomials have important applications in coding theory and are used to construct Gabidulin [Gab85] and linearised Reed-Solomon codes [Mar18]. These two families of codes are the counterpart respectively in the rank metric and in the sum-rank metric of Reed-Solomon codes [RS60], which is one of the most used families of linear codes in the Hamming metric (central since the 50's in the theory of error correction). Codes in the rank metric were first introduced by Delsarte [Del78], while those in the sum-rank metric are of more recent definition (a reference for the theory of sum-rank metric codes is [MSK22]).

Algebraic Geometry codes, a generalization of Reed-Solomon codes, where introduced by Goppa [Gop82] and are constructed by evaluating spaces of functions at rational points on algebraic curves. In [BC23] Berardini and Caruso define Linearised Algebraic Geometry codes, the first geometric construction of codes in the sum-rank metric from algebraic curves.

Let X/k be an algebraic curve (smooth, projective, geometrically connected variety of dimension one) and $K = k(X)$ be its function field. Consider the finite constant commutative k-group scheme $G = \mathbb{Z}/r\mathbb{Z}$ whose Cartier dual is $G^\vee = \mu_r = \operatorname{Spec}(k[T]/(T^r - 1))$. To give a generically free rational action of G on X is equivalent to choosing an automorphism θ of K of order r (see also Example 1.1.29). In fact, this choice defines the module algebra structure

$$\begin{aligned} k[T]/(T^r - 1) &\to \operatorname{End}_k(K) \\ T &\mapsto \theta \end{aligned}$$

corresponding to the G-action. Let $K^G = \{a \in K \mid \theta(a) = a\}$ be the subfield of fixed points and for any $x \in (K^G)^\times$ consider the μ_r-torsor

$$f_x \colon \operatorname{Spec}\left(K^G[T]/(T^r - x)\right) \to \operatorname{Spec}(K^G).$$

Then we have the smash product

$$D_{K,x} := K\#\left(K^G[T]/(T^r - x)\right) \simeq K[T;\theta]/(T^r - x)$$

and the evaluation morphism

$$\mathrm{ev}\colon D_{K,x} \to \mathrm{End}_k(K)$$

(if G is a finite commutative group scheme and $G^\vee$ its Cartier dual, one can define the smash product and ev morphism as described below given any pair of G-torsor and $G^\vee$-torsor [GH69]). Starting from this setting, *linearized Algebraic Geometry codes* are defined in [BC23]. The latter can be considered as an extension of Goppa's Algebraic Geometry codes [Gop82] to a non-commutative framework, and to the sum-rank metric. The same construction can be done for G any finite commutative k-group scheme, $G \times_k X \dashrightarrow X$ a generically free rational action and $f\colon \mathrm{Spec}(B) \to \mathrm{Spec}(K^G)$ a $G^\vee$-torsor, providing us with a larger panel of linearized Algebraic Geometry codes.

The first section of this appendix has as objective to study the endomorphisms of $B\#A$ when A is a finitely generated cocommutative bialgebra and B is a commutative A-module algebra (see Proposition A.1.4). Chase and Sweedler showed that $X = \mathrm{Spec}(B)$ is a torsor under a finite group scheme G if and only if

$$\mathrm{ev}\colon B\#k[G]^\vee \to \mathrm{End}_k(B)$$

is an isomorphism of k-algebras [CS69, Theorem 9.3]. This implies that $B\#k[G]^\vee$ is an Azumaya algebra and this holds more generally for the smash product of two Galois objects (see Theorem A.2.9 of Gamst and Hoechsmann [GH69]). Inspired by these results, in the second section we show that if A is a commutative and cocommutative Hopf algebra and B is a commutative A-module algebra via $v\colon A \to \mathrm{End}_k(B)$ such that $\ker(v)$ is a Hopf ideal of A and $A/\ker(v)$ is finite, then the smash product $B\#A$ is an Azumaya algebra over its center (that one can describe explicitly) (see Proposition A.2.11).

As seen in the main body of this work, we were particularly interested to be able of doing computations with derivations and differential operators in a greater generality. This is the main motivation that lead us to investigate smash-products: indeed, thanks to the evaluation morphism, doing computations in the algebra $\mathrm{End}_k(B)$ is the same as doing them in the smash-product algebra $B\#A$.

The last two sections of this appendix contain some results that were proven in order to better understand how to do certain computations involving derivations and differential operators: using the formalism of smash-products helped us at better understanding and having intuitions at this level. In Section A.3 we show that when dealing with A-module algebras we can always define a universal object $T(A)$ and that in $T(A)\#A$ we have some universal expressions that we can then "evaluate" in $B\#A$ for any A-module algebra B (see Corollary A.3.4). In Section A.4, we compute the reduced norm of some Ore polynomials and, as a consequence, we obtain Proposition A.4.13 which shows clearly how this helps in deducing computations involving derivations.

Let us recall the definition of the smash-product algebra Let R be a commutative ring, A be an R-bialgebra and B and C be R-algebras. If B is a (left) A-module algebra via

$$\psi\colon A \otimes_R B \to B$$

and C is a (left) A-comodule algebra via

$$\rho\colon C \to A \otimes_R C,$$

the *smash product algebra* $B\#C$ is defined as follows:

1. as an R-module $B\#C = B \otimes_R C$;
2. the multiplication is given by

$$(b \otimes c) \times (\beta \otimes \gamma) = (b \otimes 1)(\rho(c) \star \beta)(1 \otimes \gamma)$$

for any $b, \beta \in B$ and $c, \gamma \in C$.

where $f \star b := \phi(f \otimes b)$ for any $f \in A \otimes_R C$ and $b \in B$ and ϕ is the R-linear map

$$\begin{aligned}\phi\colon A \otimes_R C \otimes_R B &\to B \otimes_R C \\ a \otimes c \otimes b &\mapsto \psi(a \otimes b) \otimes c = a \cdot b \otimes c.\end{aligned}$$

One can take for example $C = A$. In this case, one can consider the *evaluation map* (the name of this map comes indeed from the coding theory setting previously discussed)

$$\begin{aligned}\mathrm{ev}\colon B\#A &\to \mathrm{End}_R(B) \\ b \otimes a &\mapsto \ell_b \circ v(a)\end{aligned}$$

where ℓ_b is the endomorphism of left multiplication by b on B and $v\colon A \to \mathrm{End}_R(B)$ defines the A-module algebra structure on B.

Lemma A.0.1. *The evaluation map defined above is a morphism of B-algebras.*

Proof. It is a direct consequence of the property (1.1) of the morphism v. □

In the following section we will encounter generalizations of the evaluation morphism obtained when considering arbitrary smash products.

A.1 Study of the endomorphisms of smash products

In this section we study the endomorphisms of $B\#A$ when A is a finitely generated cocommutative bialgebra and B is a commutative A-module algebra (see Proposition A.1.4). We start with a proposition describing all the B-algebras that are $B\#C$-modules.

Proposition A.1.1. *Let B and C be respectively (left) A-module and A-comodule algebras via*

$$v\colon A \to \mathrm{End}_R(B) \qquad \text{and} \qquad \rho\colon C \to A \otimes C,$$

D be a B-algebra and

$$u\colon B\#C \to \mathrm{End}_R(D)$$

be a B-linear map such that $u_{|C}$ is a morphism of R-algebras (where $u_{|C}$ is the composite of u with the natural map $C \to B\#C$). Then u is a morphism of left B-algebras if and only if for every $c \in C$, $b \in B$ and $d \in D$ it holds

$$u(c)(bd) = m_D(v \otimes u \circ \rho(c))(b \otimes d).$$

Proof. For every $b \in B$ we denote by ℓ_b the endomorphism of left multiplication by b on B. Now, u is a morphism of left B-algebras if and only if $u(c \times b) = u(c) \circ u(b)$ for every $c \in C$ and $b \in B$. This holds true if and only if for every $d \in D$ we have

$$u(c)(bd) = u(c) \circ \ell_b(d) = u(c) \circ u(b)(d) = u(c \times b)(d).$$

Now $c \times b = \rho(c) \star b = \sum_{i,j} v(a_i)(b)c_j$ where $\rho(c) = \sum_{i,j} a_i \otimes c_j$. Hence

$$u(c \times b)(d) = u\left(\sum_{i,j} v(a_i)(b)c_j\right)(d) = \sum_{i,j} u(v(a_i)(b)) \circ u(c_j)(d) =$$

$$\sum_{i,j} \ell_{v(a_i)(b)} \circ u(c_j)(d) = \sum_{i,j} v(a_i)(b)u(c_j)(d) = m_D(v \otimes u \circ \rho(c))(b \otimes d)$$

as claimed. □

Corollary A.1.2. *Let B and C be respectively (left) A-module and A-comodule algebras via*

$$v\colon A \to \mathrm{End}_R(B) \qquad \text{and} \qquad \rho\colon C \to A \otimes C$$

and

$$u\colon B\#C \to \mathrm{End}_R(B)$$

be a B-linear map such that $u_{|C}$ is a morphism of R-algebras. Then u is a morphism of left B-algebras if and only if for every $c \in C$ and $b, \beta \in B$ it holds

$$u(c)(b\beta) = m_B(v \otimes u \circ \rho(c))(b \otimes \beta).$$

In particular we have

$$u(c)(b) = \sum_{i,j} v(a_i)(b)u(c_j)(1) = \sum_{i,j} v(a_i)(1)u(c_j)(b)$$

for every $c \in C$ and $b \in B$ where $\rho(c) = \sum_{i,j} a_i \otimes c_j$.

Proof. Take $D = B$ in Proposition A.1.1 □

Corollary A.1.3. *Let A be a cocommutative bialgebra and B be a commutative (left) A-module algebra via $v\colon A \to \mathrm{End}_R(B)$. We then have that for every morphism of left B-algebras*

$$u\colon B\#A \to \mathrm{End}_R(B)$$

it holds

$$u(a) = \mathrm{ev}\left(\sum_{i,j} u(a_i)(1)a_j\right)$$

for every $a \in A$ where $\Delta(a) = \sum_{i,j} a_i \otimes a_j$.

Proof. By Corollary A.1.2 for every $b \in B$ it holds

$$u(a)(b) = \sum_{i,j} v(a_i)(b)u(a_j)(1) = \sum_{i,j} u(a_j)(1)v(a_i)(b) = \sum_{i,j} u(a_i)(1)v(a_j)(b)$$

where for the first equality we used the commutativity of B and for the second one the cocommutativity of A. □

Let B be an A-module algebra via $v\colon A \to \mathrm{End}_R(B)$ and $I = \ker(\varepsilon)$ be the augmentation ideal of the bialgebra A. We denote

$$B^I := \{b \in B \mid I \cdot b = 0\} = \{b \in B \mid a \cdot b = \varepsilon(a)b \quad \forall a \in A\}$$

which is an R-subalgebra of B. We then have that v factorizes via $A \to \mathrm{End}_{B^I}(B)$, indeed

$$v(a)(b) = a \cdot b = \varepsilon(a)b = bv(a)(1)$$

for every $a \in A$ and $b \in B^I$.

Proposition A.1.4. *Let A be a finitely generated cocommutative bialgebra and $\{x_1, \ldots, x_n\}$ a set of generators for A and let B be a commutative A-module algebra. There is an injection*

$$\begin{aligned}\sigma\colon \mathrm{Mor}_{\mathbf{Alg}_B}(B\#A, \mathrm{End}_{B^I}(B)) &\to \mathrm{Mor}_{\mathbf{Alg}_B}(B\#A, B\#A)\\ u &\mapsto \left(\theta_u\colon x_k \mapsto \sum_{I,J} \alpha_{IJ}^k u(x^I)(1)x^J\right)\end{aligned}$$

for $k = 1, \ldots, n$ where $\Delta(x_k) = \sum_{I,J} \alpha_{IJ}^k x^I \otimes x^J$ and x^I, x^J are monomials in $x_1, \ldots, x_n$. Moreover, σ has a left inverse given by the post-composition with the evaluation morphism $\mathrm{ev}\colon B\#A \to \mathrm{End}_{B^I}(B)$. *Finally, every endomorphism of $B\#A$ is of the form $\theta(x_k) = \sum_{I,J} \alpha_{IJ}^k u(x^I)(1)x^J \mod \ker(ev)$.*

Proof. Let $u\colon B\#A \to \mathrm{End}_{B^I}(B)$ be a morphism of B-algebras, then its image via σ is

$$\theta_u\colon x_k \mapsto \sum_{I,J} \alpha_{IJ}^k u(x^I)(1)x^J,$$

which is a morphism of algebras by definition (we define it on the generators of A and extend it to a morphism of B-algebras). Moreover, by Corollary A.1.3,

$$\mathrm{ev} \circ \theta_u(x_k) = \mathrm{ev}\left(\sum_{I,J} \alpha_{IJ}^k u(x^I)(1)x^J\right) = u(x_k)$$

for every $k = 1, \dots, n$ that is composing by ev is a left inverse of σ and σ is an injection. Now, let $\theta \in \mathrm{End}_B(B\#A)$ and write $\theta(x_k) = \sum_S \gamma_S x^S$. Since $\mathrm{ev}\colon B\#A \to \mathrm{End}_{B^I}(B)$ is a morphism of B-algebras, the composite $u_\theta = \mathrm{ev} \circ \theta$ is a morphism of B-algebras, that is, by Corollary A.1.3,

$$u_\theta(x_k) = \mathrm{ev}\left(\sum_{I,J} \alpha_{IJ}^k u(x^I)(1)x^J\right)$$

but also

$$u_\theta(x_k) = \mathrm{ev} \circ \theta(x_k) = \mathrm{ev}\left(\sum_S \gamma_S x^S\right)$$

and the claim follows. □

Corollary A.1.5. *Consider the Hopf algebra $A = k\left[T, \frac{1}{T}, S\right]$ with $\Delta(T) = T \otimes T$ and $\Delta(S) = S \otimes 1 + T \otimes S$ and let K be a field extension of k along with an automorphism θ and a θ-derivation $\partial\colon K \to K$ (which define on K an A-module algebra structure). Then $K\#k\left[T, \frac{1}{T}, S\right]$ contains the algebra of Ore polynomials $K[S; \theta, \partial]$ (see Example 1.1.29) and*

$$u\colon K\#k\left[T, \frac{1}{T}, S\right] \to \mathrm{End}_k(K)$$

is a morphism of K-algebras if and only if $u(T) = c\theta$ and $u(S) = \partial + c'\theta$ for some constants $c, c' \in K$.

Proof. By Corollary A.1.2 we know that for every morphism of K-algebras

$$u\colon K\#k\left[T, \frac{1}{T}, S\right] \to \mathrm{End}_k(K)$$

it holds

$$u(T)(x) = \theta(x)u(T)(1)$$

and

$$u(S)(x) = \partial(x) + \theta(x)u(S)(1)$$

for every $x \in K$, hence the statement. □

These kind of morphisms are studied and used in the context or Reed-Solomon codes, see for example [CD23].

A.2 Smash products and Azumaya algebras

We start this section by recalling some known facts about central simple algebras and Azumaya algebras. As a reference for central simple algebras and Azumaya algebra we refer to the books [GS06] and [Mil80]. Let k be a field.

Definition A.2.1 (Central simple algebra)**.** A finite-dimensional k-algebra A is called *simple* if it does not have non-trivial two-sided ideals. A *central simple k-algebra* is a simple k-algebra A whose center is exactly k.

Fact A.2.2.

- The center of any simple algebra is a field. Therefore any simple algebra is a central simple algebra over its center.
- Let A be a central simple k-algebra. Then there exists a finite separable extension L/k such that $A \otimes_k L \simeq M_n(L)$. Therefore one can consider the following composite

$$N_{rd}\colon A \hookrightarrow A \otimes_k L \simeq M_n(L) \overset{\det}{\to} L.$$

  The image of N_{rd} lies in k, moreover N_{rd} depends neither on the choice of L nor on the isomorphism $A \otimes_k L \simeq M_n(L)$. We then have a well-defined map

$$N_{rd}\colon A \to k$$

  called *reduced norm*.

Let R be a commutative ring.

Definition A.2.3 (Azumaya algebra)**.** A finite locally free R-algebra A is said to be an *Azumaya algebra* if $A \otimes_R \mathrm{Frac}(R/\mathfrak{p})$ is a central simple $\mathrm{Frac}(R/\mathfrak{p})$-algebra for every $\mathfrak{p} \in \mathrm{Spec}(R)$.

There is a well-defined notion of reduced norm also for Azumaya algebras (see [Sal80]). Azumaya algebras are also sometimes referred to as *central separable algebras* (see for example [AG60] and [DI71]). For what concerns the *reduced norm*, it was defined in [EW67] and has some foundation in the work of Goldman [Gol61] on determinants for projective modules. Let Λ be an Azumaya algebra over a commutative ring R. Then there exist S a commutative R-algebra and P a finitely generated, faithful, projective S-module such that $\Lambda \otimes_R S \simeq \mathrm{Hom}_S(P, P)$. Such an S is called *splitting ring* for Λ and it is called *proper* if $R \subseteq S$. Via the isomorphism $\Lambda \otimes_R S \simeq \mathrm{End}_S(P)$ we can compute a characteristic polynomial (trace and discriminant) for any element of Λ and one sees that they do not depend on the choice of S, P or the isomorphism (see [EW67, Proposition 3.1]). These are what we will call *reduced* characteristic polynomial, trace and norm.

Let us recall the definition of a torsor under the action of a group scheme and of its algebraic counterpart, Galois objects. Let S be a scheme, G be an S-group scheme and $X \to Y$ be a (right) *G-torsor*, that is

$$\begin{aligned} X \times_S G &\to X \times_Y X \\ (x, g) &\mapsto (x, x \cdot g) \end{aligned}$$

is an isomorphism. More explicitly, if we denote by $\rho\colon X \times_S G \to X$ the (right) action of G on X, the isomorphism is given by the composite

$$X \times_S G \overset{diag\times id}{\longrightarrow} X \times_Y X \times_S G \overset{id\times\rho}{\longrightarrow} X \times_Y X.$$

If we are in the affine case, with $S = \mathrm{Spec}(R)$ for R a commutative ring, $G = \mathrm{Spec}(A)$ for A an R-Hopf algebra, $X = \mathrm{Spec}(B)$ for B a C-algebra, $Y = \mathrm{Spec}(C)$ and we still denote by $\rho\colon B \to B \otimes_R A$ the corresponding co-action, then the above isomorphism is equivalent to saying that the following composite is an isomorphism of R-algebras (and even of B-algebras)

$$B \otimes_C B \overset{id\otimes\rho}{\longrightarrow} B \otimes_C B \otimes_R A \overset{m_B\otimes id}{\longrightarrow} B \otimes_R A$$

and we say that B is an *A-Galois object*. When A and B are finite locally free over R, then we have the following isomorphisms given by adjunction:

$$\mathrm{Hom}_{\mathbf{Alg}_R}(B, B \otimes_R A) \simeq \mathrm{Hom}_{\mathbf{Alg}_R}(B, \mathrm{Hom}_R(A^\vee, B)) \simeq$$

$$\{v\colon A^\vee \to \mathrm{End}_R(B) \text{ with property A.1}\}$$

$$\begin{cases} v(\varphi)(1) = \varepsilon(\varphi) \\ v(\varphi)(fg) = m_B(v \otimes v \circ \Delta(a))(f \otimes g) \end{cases} \tag{A.1}$$

and

$$\{\rho\colon B \to B\otimes_R A \text{ structure of } A\text{-comodule }\} \simeq \{\psi\colon A^\vee\otimes_R B \to B \text{ structure of } A^\vee\text{-modules}\}$$

$$\simeq \mathrm{Hom}_{\mathbf{Alg}_R}(A^\vee, \mathrm{End}_R(B)).$$

Corollary A.2.4. *We have the following natural bijection:*

$$\{(m_B\otimes id)\circ(id\otimes\rho)\colon B\otimes_R B \to B\otimes_R A \mid \rho\colon B \to B\otimes_R A \textit{ structure of } A\textit{-comodule algebra}\}$$

$$\simeq \{\mathrm{ev} = id \otimes v\colon B\#A^\vee \to \mathrm{End}_R(B) \mid \textit{morphisms of algebras}\}.$$

Remark A.2.5. From the above result, we deduce that when we are looking at an A-module algebra B, the right requirement that plays the counterpart of being a torsor or a Galois object is asking that

$$\mathrm{ev}\colon B\#A \to \mathrm{End}_{B^I}(B)$$

is an isomorphism. We have in fact the following result:

Theorem A.2.6. *Let A be a finite locally free commutative R-Hopf algebra and B be a commutative A-comodule algebra (that is there is an action of* $\mathrm{Spec}(A)$ *on* $\mathrm{Spec}(B)$*). Then the following are equivalent:*

1. *B is a Galois A-object (that is* $\mathrm{Spec}(B)$ *is a* $\mathrm{Spec}(A)$*-torsor);*

2. *B is a finitely generated faithful projective R-module and the evaluation map*

$$\mathrm{ev}\colon B\#A^\vee \to \mathrm{End}_R(B)$$

is an isomorphism of R-algebras.

If the above conditions hold true, then B is both a projective left $D = B\#A^\vee$-module and a projective left $A^\vee$-module and $D^A := \{w \in D \mid 1 \otimes a \times w = \varepsilon(a)w \quad \forall a \in A\} = JD$ where $J = A^{\vee A^\vee} := \{x \in A^\vee \mid fx = \varepsilon(f)x \quad \forall f \in A^\vee\} = \mathrm{Ann}(\ker \varepsilon_{A^\vee})$.

Proof. See [CS69, Theorem 9.3 and 9.6]. □

Corollary A.2.7. *Let A be a finite locally free commutative R-Hopf algebra and B be a commutative A-comodule algebra. If B is a Galois A-object, then $B\#A^\vee$ is an Azumaya algebra.*

Lemma A.2.8. *Let S be an R-algebra. Then*

$$\phi\colon (B\#C) \otimes_R S \to (B \otimes_R S)\#(C \otimes_R S)$$
$$b \otimes c \otimes 1 \mapsto b \otimes 1 \otimes c \otimes 1$$

is an isomorphism of S-algebras.

Proof. First of all let us show that ϕ is a morphism of algebras: for any $b, \beta \in B$ and $c, \gamma \in C$

$$\phi((b \otimes c \otimes 1) \times (\beta \otimes \gamma \otimes 1)) = \phi(\sum ba_i \cdot \beta \otimes c_i\gamma \otimes 1) =$$

$$\sum ba_i \cdot \beta \otimes 1 \otimes c_i\gamma \otimes 1 = (b \otimes 1 \otimes c \otimes 1) \times (\beta \otimes 1 \otimes \gamma \otimes 1)$$

where we wrote $\rho_C(c) = \sum a_i \otimes c_i$. Moreover the two objects are isomorphic as S-modules via ϕ since

$$B \otimes_R S \otimes_S A \otimes_R S \simeq B \otimes_R A \otimes_R S,$$

so they are also isomorphic as algebras. □

Theorem A.2.9 ([GH69])**.** *Let R be a commutative ring, A be a commutative finite locally free R-Hopf algebra, B be a commutative finite locally free (right) $A^\vee$-Galois object over R and C be a commutative finite locally free (left) A-Galois object over R. Then the smash product $B\#C$ is an Azumaya algebra over R, in particular $(B\#C) \otimes_R C$ and $\mathrm{End}_C(B \otimes_R C)$ are isomorphic as C-algebras.*

Proof. This is a known result for $C = A$ the trivial torsor (by Corollary A.2.7): in this case $B\#A \simeq \mathrm{End}_R(B)$ as R-algebras. Now, being C a (left) A-Galois object, $C \otimes_R C \simeq A \otimes_R C$ thus

$$(B\#C) \otimes_R C \simeq (B \otimes_R C)\#(C \otimes_R C) \simeq (B \otimes_R C)\#(A \otimes_R C) \simeq \mathrm{End}_C(B \otimes_R C)$$

where the first isomorphism holds true by Lemma A.2.8 and for the last isomorphism we used the trivial-torsor case. □

Our objective is to show that $B\#A$ is an Azumaya algebra over its center under some less restrictive hypothesis. The setting will be the following: let A be a commutative and cocommutative R-Hopf algebra, B a commutative A-module algebra via $v\colon A \to \mathrm{End}_R(B)$ such that $A/\ker(v)$ is a finite locally free Hopf algebra and denote $H = \mathrm{Spec}\,(A/\ker(v))$. Suppose moreover that B is a (right) $(A/\ker(v))^\vee \otimes_R B^I$-Galois object over B^I, where $B^I = \{b \in B \mid I \cdot b = 0\}$ and I denotes the augmentation ideal of A. Notice moreover that A is a (left) $A^H \otimes_R A/\ker(v)$-Galois object over A^H via

$$\overline{\Delta}\colon A \xrightarrow{\Delta} A \otimes_R A \to A/\ker(v) \otimes_R A,$$

where $A^H = \{a \in A \mid a \mapsto 1 \otimes a, \quad A \xrightarrow{\Delta} A \otimes_R A \to A/\ker(v) \otimes_R A\}$ represents the quotient $\mathrm{Spec}(A)/H$.

Now, we want to do appropriate base changes in order to have a common base ring: $B \otimes_R A^H$ is a (right) $(A/\ker(v))^\vee \otimes_R B^I \otimes_R A^H$-Galois object over $B^I \otimes_R A^H$ and $B^I \otimes_R A$ is a (left) $B^I \otimes_R A^H \otimes_R A/\ker(v)$-Galois object over $B^I \otimes_R A^H$.

Therefore, we can consider the smash product $(B \otimes_R A^H)\#(B^I \otimes_R A)$.

Lemma A.2.10. *In the above setting, $(B \otimes_R A^H)\#(B^I \otimes_R A)$ and $B\#A$ are isomorphic as $(B^I \otimes_R A^H)$-algebras.*

Proof. We claim that the isomorphism is given by

$$\begin{aligned} \psi\colon B\#A &\to (B \otimes_R A^H)\#(B^I \otimes_R A) \\ b \otimes a &\mapsto (b \otimes 1) \otimes (1 \otimes a), \\ b\beta \otimes a\alpha &\leftarrow\!\shortmid (b \otimes a) \otimes (\beta \otimes \alpha). \end{aligned}$$

First of all notice that for $a \in A$ and $\beta \in B$ it holds $\Delta(a) \star \beta = \overline{\Delta}(a) \star \beta$ since $\overline{\Delta}$ is defined by going modulo $\ker(v)$ on the left and $x \cdot \beta = 0$ for all $x \in \ker(v)$. This is all we need to see that the morphism we defined is a morphism of R-algebras. Indeed, if we write $\overline{\Delta}(a) = \sum a_{ij} e_i \otimes e_j$, then we have

$$(b \otimes a) \times (\beta \otimes \alpha) = \sum a_{ij} b e_i \cdot \beta \otimes e_j \alpha$$

and thus

$$\psi((b \otimes a) \times (\beta \otimes \alpha)) = \sum a_{ij} b e_i \cdot \beta \otimes 1 \otimes 1 \otimes e_j \alpha.$$

Moreover

$$\psi(b \otimes a) \times \psi(\beta \otimes \alpha) = (b \otimes 1 \otimes 1 \otimes a) \times (\beta \otimes 1 \otimes 1 \otimes \alpha) =$$

$$(m_B \otimes \mathrm{ev} \otimes m_A) \circ (\mathrm{id} \otimes \rho_B \otimes \overline{\Delta} \otimes \mathrm{id})(b \otimes 1 \otimes \beta \otimes 1 \otimes 1 \otimes a \otimes 1 \otimes \alpha) =$$

$$(m_B \otimes \mathrm{ev} \otimes m_A)(b \otimes 1 \otimes (\sum e_i \cdot \beta \otimes 1 \otimes e_i^\vee \otimes 1) \otimes (\sum a_{ij} 1 \otimes e_i \otimes 1 \otimes e_j) \otimes 1 \otimes \alpha) =$$

$$\sum a_{ij} b e_i \cdot \beta \otimes 1 \otimes 1 \otimes e_j \alpha$$

as wished. To show that the two maps are mutually inverse, notice that one way it is immediate. For the other way around, since $(B \otimes_R A^H)\#(B^I \otimes_R A)$ is a $B^I \otimes_R A^H$-algebra, then we have

$$(b \otimes a) \otimes (\beta \otimes \alpha) = (\beta \otimes a)(b \otimes 1 \otimes 1 \otimes \alpha) = b\beta \otimes 1 \otimes 1 \otimes a\alpha$$

that shows that the second map is a right inverse of ψ. This also proves that ψ is $B^I \otimes_R A^H$-linear and thus the statement is proved. □

Proposition A.2.11. *The smash product $B\#A$ is an Azumaya algebra over $B^I \otimes_R A^H$, which is its center. In particular*

$$(B\#A) \otimes_{B^I \otimes_R A^H} (B^I \otimes_R A) \simeq \mathrm{End}_{B^I \otimes_R A}(B \otimes_R A)$$

and

$$(B \otimes_R A^H) \otimes_{B^I \otimes_R A^H} (B\#A) \simeq \mathrm{End}_{B \otimes_R A^H}(B \otimes_R A).$$

Proof. This is immediate by applying Theorem A.2.9 to $(B \otimes_R A^H)\#(B^I \otimes_R A)$ and using the isomorphism of the Lemma A.2.10. □

This result provides us with a reduced norm.

Definition A.2.12 (Reduced norm)**.** Consider the following composite:

$$B\#A \hookrightarrow (B\#A) \otimes_{B^I \otimes_R A^H} (B^I \otimes_R A) \simeq \mathrm{End}_{B^I \otimes_R A}(B \otimes_R A) \stackrel{det}{\to} B^I \otimes_R A.$$

By results on Azumaya algebras (see for example [EW67]), this composite does not depend neither on the trivialization nor on the isomorphism and moreover it factorizes via $B^I \otimes_R A^H$. So considering the composite

$$B\#A \hookrightarrow (B \otimes_R A^H) \otimes_{B^I \otimes_R A^H} (B\#A) \simeq \mathrm{End}_{B \otimes_R A^H}(B \otimes_R A) \stackrel{det}{\to} B \otimes_R A^H$$

gives the same image of a chosen element $b \otimes a$ in the smash product $B\#A$. We call *reduced norm* the map

$$N_{rd} \colon B\#A \to B^I \otimes_R A^H$$

obtained.

Lemma A.2.13. *For any element $b \otimes a$ in the smash product $B\#A$, its image through the isomorphism*

$$(B\#A) \otimes_{B^I \otimes_R A^H} (B^I \otimes_R A) \simeq \mathrm{End}_{B^I \otimes_R A}(B \otimes_R A)$$

is the endomorphism $\ell_{b\otimes a}$ of multiplication on the left by $b \otimes a$, while via

$$(B \otimes_R A^H) \otimes_{B^I \otimes_R A^H} (B\#A) \simeq \mathrm{End}_{B \otimes_R A^H}(B \otimes_R A)$$

is the endomorphism $r_{b\otimes a}$ of multiplication on the right by $b \otimes a$.

Proof. Let us write explicitly the image of an element $b \otimes a$ in the smash product $B\#A$ through the isomorphisms of Proposition A.2.11. In the first case we have:

$$\begin{array}{ccc} (B\#A) \otimes_{B^I \otimes_R A^H} (B^I \otimes_R A) & \overset{A.2.10}{\simeq} & \big((B \otimes_R A^H)\#(B^I \otimes_R A)\big) \otimes_{B^I \otimes_R A^H} (B^I \otimes_R A) \\ b \otimes a \otimes 1 \otimes 1 & \mapsto & (b \otimes 1) \otimes (1 \otimes a) \otimes (1 \otimes 1) \end{array}$$

$$\begin{array}{ccc} & \overset{A.2.8}{\simeq} & \big((B \otimes_R A^H) \otimes_{B^I \otimes_R A^H} (B^I \otimes_R A)\big) \# \big((B^I \otimes_R A) \otimes_{B^I \otimes_R A^H} (B^I \otimes_R A)\big) \\ & \mapsto & (b \otimes 1) \otimes (1 \otimes 1) \otimes (1 \otimes a) \otimes (1 \otimes 1) \end{array}$$

$$\begin{array}{ccc} & \overset{A.2.10+torsor}{\simeq} & (B \otimes_R A)\# \big(\big(B^I \otimes_R A^H \otimes_R A/\ker(v)\big) \otimes_{B^I \otimes_R A^H} (B^I \otimes_R A)\big) \\ & \mapsto & \textstyle\sum_{i,j} (b \otimes 1) \otimes (1 \otimes 1 \otimes \overline{a_i}) \otimes (1 \otimes a_j) \\ & \overset{ev}{\simeq} & \mathrm{End}_{B^I \otimes_R A}(B \otimes_R A) \\ & \mapsto & (\beta \otimes \alpha \mapsto \textstyle\sum_{i,j} b(\overline{a_i} \cdot \beta) \otimes a_j \alpha) \end{array}$$

where we wrote $\overline{\Delta}(a) = \sum_{i,j} \overline{a_i} \otimes a_j$. Notice that

$$\sum_{i,j} b(\overline{a_i} \cdot \beta) \otimes a_j \alpha = (b \otimes a) \cdot (\beta \otimes \alpha) = \ell_{b \otimes a}(\beta \otimes \alpha),$$

so the first statement holds true.

On the other hand, using the second trivialization we obtain:

$$\begin{array}{ccc} (B \otimes_R A^H) \otimes_{B^I \otimes_R A^H} (B\#A) & \overset{A.2.10}{\simeq} & (B \otimes_R A^H) \otimes_{B^I \otimes_R A^H} \big((B \otimes_R A^H)\#(B^I \otimes_R A)\big) \\ 1 \otimes 1 \otimes b \otimes a & \mapsto & (1 \otimes 1) \otimes (b \otimes 1) \otimes (1 \otimes a) \end{array}$$

$$\begin{array}{ccc} & \overset{A.2.8}{\simeq} & \big((B \otimes_R A^H) \otimes_{B^I \otimes_R A^H} (B \otimes_R A^H)\big) \# \big((B \otimes_R A^H) \otimes_{B^I \otimes_R A^H} (B^I \otimes_R A)\big) \\ & \mapsto & (1 \otimes 1) \otimes (b \otimes 1) \otimes (1 \otimes 1) \otimes (1 \otimes a) \end{array}$$

$$\begin{array}{ccc} & \overset{A.2.10+torsor}{\simeq} & \big((B \otimes_R A^H) \otimes_{B^I \otimes_R A^H} \big((A/\ker(v))^\vee \otimes_R B^I \otimes_R A^H\big)\big) \#(B \otimes_R A) \\ & \mapsto & \textstyle\sum_i (e_i \cdot b \otimes 1) \otimes (e_i^* \otimes 1 \otimes 1) \otimes (1 \otimes a) \end{array}$$

$$\overset{ev}{\simeq} \qquad \mathrm{End}_{B\otimes_R A^H}(B\otimes_R A)$$

$$\mapsto \quad (\beta\otimes\alpha \mapsto \textstyle\sum_i \beta(e_i\cdot b)\otimes(e_i^*\cdot\alpha)a).$$

Recall that the relation between the $A/\ker(v)$-comodule structure

$$\overline{\Delta}\colon A\to A/\ker(v)\otimes_R A$$

and the $(A/\ker(v))^\vee$-module structure

$$A\otimes_R (A/\ker(v))^\vee \to A$$

is given by $\overline{\Delta}(\alpha)=\sum e_i\otimes e_i^*\alpha$ for every $\alpha\in A$, where $\{e_i\}$ is a fixed base of the finite algebra $A/\ker(v)$. We then have

$$r_{b\otimes a}(\beta\otimes\alpha)=(\beta\otimes\alpha)\cdot(b\otimes a)=(\beta\otimes 1)(\Delta(\alpha)*b)(1\otimes a)$$
$$=(\beta\otimes 1)(\overline{\Delta}(\alpha)*b)(1\otimes a)=\sum_i \beta(e_i\cdot b)\otimes(e_i^*\cdot\alpha)a$$

as stated. □

Corollary A.2.14. *The reduced norm $N_{rd}\colon B\#A\to B^I\otimes_R A^H$ coincides with the classical norm $N_{(B\#A)/C}\colon x\mapsto\det(m_x)$ where m_x is the matrix associated to the endomorphism of multiplication by x and C can be either $B^I\otimes_R A$ or $B\otimes_R A^H$.*

Proof. This is a direct consequence of the previous Lemma. □

A.3 Universal object in the category of module algebras

In this section we show that when dealing with A-module algebras we can always define a universal object $T(A)$ and that in $T(A)\#A$ we have some universal expressions that we can then "evaluate" in $B\#A$ for any A-module algebra B (see Corollary A.3.4). This can be helpful in order to doing computations in any smash-product algebra and, as a consequence, in the algebra $\mathrm{End}_k(B)$.

Proposition A.3.1. *Let R be a commutative ring, A an R-bialgebra and V an A-module via $\nu\colon A\to\mathrm{End}_R(V)$. Then the tensor algebra $T(V)$ of V as R-module has a natural structure of A-module algebra.*

Proof. Let

$$\eta\colon V\to\mathrm{Hom}_R(A,V)$$
$$v\mapsto(a\mapsto a\cdot v).$$

be the R-linear morphism corresponding to the A-module structure on V and consider the natural inclusion

$$\mathrm{Hom}_R(A,V)\hookrightarrow\mathrm{Hom}_R(A,T(V)).$$

Then, since $\mathrm{Hom}_R(A, T(V))$ is an associative algebra, by the universal property of the tensor algebra the composite $V \xrightarrow{\eta} \mathrm{Hom}_R(A, V) \hookrightarrow \mathrm{Hom}_R(A, T(V))$ factors naturally through a morphism of algebras

$$T(V) \to \mathrm{Hom}_R(A, T(V))$$

which corresponds also to

$$\nu' \colon A \to \mathrm{End}_R(T(V))$$

extending ν and respecting the property of compatibility with products (1.1). We wish to see that ν' is also a morphism of algebras. It is enough to show it for elementary tensors $v_1 \otimes \cdots \otimes v_k$, moreover, once shown for $v_1 \otimes v_2$, the general case follows by induction. Take a_1, a_2 in A and call $\alpha = a_1 a_2$. Let $\Delta(a_k) = \sum_{i,j} a_{ki} \otimes a_{kj}$ for $k = 1, 2$. Then

$$\Delta(\alpha) = \Delta(a_1)\Delta(a_2) = \sum_{i,j,s,t} a_{1i}a_{2s} \otimes a_{1j}a_{2t}$$

and thus, by compatibility with products,

$$\nu'(\alpha)(v_1 \otimes v_2) = \nu'(\alpha)(v_1 \otimes 1 \cdot 1 \otimes v_2) = \sum_{i,j,s,t} \nu'(a_{1i}a_{2s})(v_1) \otimes \nu'(a_{1j}a_{2t})(v_2) =$$

$$\sum_{i,j,s,t} \nu'(a_{1i})(\nu'(a_{2s})(v_1)) \otimes \nu'(a_{1j})(\nu'(a_{2t})(v_2)) =$$

$$\nu'(a_1)\left(\sum_{s,t} \nu'(a_{2s})(v_1) \otimes \nu'(a_{2t}(v_2))\right) = \nu'(a_1) \circ \nu'(a_2)(v_1 \otimes v_2).$$

Therefore $T(V)$ has a natural structure of A-module algebra □

Remark A.3.2. If A is cocommutative then it holds that the symmetric algebra $Sym(V)$ has a natural structure of A-module algebra. Indeed the image of

$$V \xrightarrow{\eta} \mathrm{Hom}_R(A, V) \hookrightarrow \mathrm{Hom}_R(A, Sym(V))$$

is commutative since for any $v, w \in V$

$$\eta(w) * \eta(v) = m_V \circ \eta(v) \otimes \eta(w) \circ \tau \circ \Delta_A$$

(using the fact that multiplication in V is commutative) and by cocommutativity of A the diagram

$$A \xrightarrow{\Delta_A} A \otimes_R A \xrightarrow{\tau} A \otimes_R A \xrightarrow{\eta(v)\otimes\eta(w)} V \otimes_R V \xrightarrow{m_V} V$$

$$A \xrightarrow{\Delta_A} A \otimes_R A$$

commutes, that is $\eta(w) * \eta(v) = \eta(v) * \eta(w)$. Hence, by the universal property of the symmetric algebra, we obtain naturally a morphism of algebras

$$Sym(V) \to \mathrm{Hom}_R(A, Sym(V))$$

corresponding to

$$A \to \mathrm{End}_R(Sym(V))$$

which, as above, is seen to be a morphism of algebras too.

The following proposition shows that $T(A)$ is a universal object in the category of A-module algebras.

Proposition A.3.3. *The functor $T\colon \mathrm{Mod}_A \to \mathrm{ModAlg}_A$ from the category of A-modules to that of A-module algebras is left adjoint to the forgetful functor.*

Proof. This is a direct consequence of the fact that the tensor algebra functor $T\colon \mathrm{Mod}_A \to \mathrm{Alg}_A$ is left adjoint to the forgetful functor and that morphisms of A-module algebras are just morphisms of A-algebras (see Remark 1.1.17). □

Notice that in particular we have the natural isomorphism

$$\begin{aligned} \mathrm{Hom}_{\mathrm{ModAlg}_A}(T(A), B) &\to B \\ \varphi &\mapsto \varphi(1) \\ (\varphi_b\colon a \mapsto a \cdot b) &\leftarrow\!\shortmid b. \end{aligned}$$

Applying Proposition 1.1.25 we obtain directly the following:

Corollary A.3.4. *For every A-module algebra B and $b \in B$,*

$$\varphi_b \otimes id\colon T(A)\#A \to B\#A$$

is a morphism of algebras.

The above statement is useful in order to have some "universal expressions" when doing computations in $B\#A$ for any choice of an A-module algebra B.

Proposition A.3.5. *Let A be a cocommutative R-bialgebra. Then we have a morphism of algebras*

$$Sym(A)\#A \to Sym(A \otimes_R A)\#A \otimes_R A$$

induced by the comultiplication Δ of A.

Proof. By the universal property of $Sym(A)$, the morphism $\Delta\colon A \to A \otimes_R A$ extends naturally to a morphism of algebras

$$\widetilde{\Delta}\colon Sym(A) \to Sym(A \otimes_R A).$$

Endowing $Sym(A \otimes_R A)$ with the $A \otimes_R A$-module algebra structure induced by the multiplication, we have that $\widetilde{\Delta}$ is a morphism of module algebras with respect to $\Delta\colon A \to A \otimes_R A$, indeed the diagram

$$\begin{array}{ccc} A \otimes_R Sym(A) & \xrightarrow{\widetilde{m_A}} & Sym(A) \\ \downarrow{\scriptstyle \Delta\otimes\widetilde{\Delta}} & & \downarrow{\scriptstyle \widetilde{\Delta}} \\ A \otimes_R A \otimes_R Sym(A \otimes_R A) & \xrightarrow{\widetilde{m_{A\otimes_R A}}} & Sym(A \otimes_R A) \end{array}$$

commutes (we just use the fact that Δ is a morphism of algebras), where $\widetilde{m_A}$ and $\widetilde{m_{A\otimes_R A}}$ are respectively the A-module algebra and the $A \otimes_R A$-module algebra structures induced by the respective multiplications on $Sym(A)$ and on $Sym(A \otimes_R A)$. Moreover, $\Delta\colon A \to A \otimes_R A$ is a morphisms of comodule algebras (with respect to Δ) where the comodule structures are given by Δ on A and by $\Delta_{A\otimes_R A}$ on $A \otimes_R A$ (we recall that $\Delta_{A\otimes_R A} = \tau_{23} \circ \Delta \otimes \Delta$ where τ_{23} switches the elements in second and third position in an elementary tensor, see Remark 1.1.5), indeed the diagram

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_R A \\ \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle \Delta_{A\otimes_R A}} \\ A \otimes_R A & \xrightarrow{\Delta\otimes\Delta} & A \otimes_R A \otimes_R A \otimes_R A \end{array}$$

commutes (we use the fact that A is cocommutative). We then have, by Proposition 1.1.25, that

$$\widetilde{\Delta} \otimes \Delta\colon Sym(A)\#A \to Sym(A \otimes_R A)\#A \otimes_R A$$

is a morphism of algebras. □

The case of Ore polynomials

Let R be a commutative ring of characteristic p, $A = R[X]$ with $\Delta(X) = X \otimes 1 + 1 \otimes X$. Then $Sym(A) = R\left[\widetilde{X^i}\right]_{i\geq 0}$ and it is an A-module algebra where the structure is induced by the multiplication of A on itself, that is, it corresponds to the derivation

$$\begin{aligned} Sym(A) &\to Sym(A) \\ \widetilde{X^i} &\mapsto \widetilde{X^{i+1}}. \end{aligned}$$

Lemma A.3.6. *Let us give to every $\widetilde{X^i}$ weight i for all $i \geq 0$. Then $Sym(A)\#A$ is a graded ring where the grading is given by homogeneous polynomials of degree d in $X, \widetilde{X^i}$ for $i \geq 0$.*

Proof. We just need to verify that the gradation is respected by products but this is okay since

$$X\widetilde{X^i} = \widetilde{X^{i+1}} + \widetilde{X^i}X$$

for every $i \geq 0$. □

Corollary A.3.7. *Products of homogeneous polynomials in $Sym(A)\#A$ are homogeneous (of degree the sum of the degrees of the factors).*

Definition A.3.8 (Additive polynomial)**.** We say that a polynomial $Q(X, \widetilde{X^i})_{i\geq 0}$ in $Sym(A)\#A$ is *additive* if

$$Q(\Delta(X), \widetilde{\Delta}(\widetilde{X^i}))_{i\geq 0} = Q(X\otimes 1, \widetilde{X^i\otimes 1})_{i\geq 0} + Q(1\otimes X, \widetilde{1\otimes X^i})_{i\geq 0}.$$

Lemma A.3.9. *A polynomial $Q(X, \widetilde{X^i})_{i\geq 0}$ in $Sym(A)\#A$ is additive if and only if it is of the form*

$$\sum_{k\geq 0} a_k X^{p^k} + \sum_{s,t\geq 0} a_{st}\left(\widetilde{X^{p^s}}\right)^{p^t} \tag{A.2}$$

where the coefficients are in R.

Proof. The if part is clear by the definition of the comultiplication. For the converse, it suffices to show the claim for monomials and again using the definition of the comultiplication it is clear that the only additive monomials are those of the form appearing in (A.2). □

Proposition A.3.10. *In $Sym(A)\#A$ we have $(X+\widetilde{X})^{p^k} = X^{p^k} + \sum_{j=0}^{k}\left(\widetilde{X^{p^j}}\right)^{p^{k-j}}$ for every integer $k\geq 0$.*

Proof. First of all remark that the polynomial $Q(X, \widetilde{X^i})_{i\geq 0} = (X+\widetilde{X})^{p^k}$ is homogeneous of degree p^k in the variables $X, \widetilde{X}, \ldots, \widetilde{X^{p^k}}$. Let us show that Q is additive. By Proposition A.3.5, $\widetilde{\Delta}\otimes\Delta$ is a morphism of rings, therefore

$$Q(\Delta(X), \widetilde{\Delta}(\widetilde{X}), \ldots, \widetilde{\Delta}(\widetilde{X^{p^k}})) = (\widetilde{\Delta}\otimes\Delta)((X+\widetilde{X})^{p^k}) =$$

$$((\widetilde{\Delta}\otimes\Delta)(X+\widetilde{X}))^{p^k} = (X\otimes 1 + 1\otimes X + \widetilde{X\otimes 1} + \widetilde{1\otimes X})^{p^k}.$$

Now, $X\otimes 1 + \widetilde{X\otimes 1}$ and $1\otimes X + \widetilde{1\otimes X}$ commute, indeed

$$(X\otimes 1+\widetilde{X\otimes 1})(1\otimes X+\widetilde{1\otimes X}) = X\otimes X+X\otimes 1\cdot\widetilde{1\otimes X}+(\widetilde{X\otimes 1})(1\otimes X)+(\widetilde{X\otimes 1})(\widetilde{1\otimes X}) =$$

$$X\otimes X + (X\otimes 1\otimes 1\otimes 1 + 1\otimes 1\otimes X\otimes 1)\star\widetilde{1\otimes X} + (\widetilde{X\otimes 1})(1\otimes X) + (\widetilde{X\otimes 1})(\widetilde{1\otimes X}) =$$

$$X\otimes X + \widetilde{X\otimes X} + (\widetilde{1\otimes X})(X\otimes 1) + (\widetilde{X\otimes 1})(1\otimes X) + (\widetilde{X\otimes 1})(\widetilde{1\otimes X})$$

while

$$(1\otimes X+\widetilde{1\otimes X})(X\otimes 1+\widetilde{X\otimes 1}) = X\otimes X+1\otimes X\cdot\widetilde{X\otimes 1}+(\widetilde{1\otimes X})(X\otimes 1)+(\widetilde{1\otimes X})(\widetilde{X\otimes 1}) =$$

$$X\otimes X + (1\otimes X\otimes 1\otimes 1 + 1\otimes 1\otimes 1\otimes X)\star\widetilde{X\otimes 1} + (\widetilde{1\otimes X})(X\otimes 1) + (\widetilde{1\otimes X})(\widetilde{X\otimes 1}) =$$

$$X\otimes X + \widetilde{X\otimes X} + (\widetilde{X\otimes 1})(1\otimes X) + (\widetilde{1\otimes X})(X\otimes 1) + (\widetilde{1\otimes X})(\widetilde{X\otimes 1}).$$

Therefore

$$(X\otimes 1 + 1\otimes X + \widetilde{X\otimes 1} + \widetilde{1\otimes X})^{p^k} = (X\otimes 1 + \widetilde{X\otimes 1})^{p^k} + (1\otimes X + \widetilde{1\otimes X})^{p^k} =$$

$$Q(X \otimes 1, \widetilde{X \otimes 1}, \ldots, \widetilde{X^{p^k} \otimes 1}) + Q(1 \otimes X, \widetilde{1 \otimes X}, \ldots, \widetilde{1 \otimes X^{p^k}})$$

that is Q is an additive polynomial. By Lemma A.3.9 and by degree reasons we then have that Q must be of the form

$$aX^{p^k} + \sum_{j=0}^{k} a_j \left(\widetilde{X^{p^j}}\right)^{p^{k-j}}$$

where the coefficients are in R. One can easily see that all the coefficients are 1. □

Corollary A.3.11. *Let $Z(T) = T^{p^r} + z_{r-1}T^{p^{r-1}} + \ldots z_1T^p + z_0T$ be any linearised polynomial with coefficients in R. Then in $Sym(A)\#A$ it holds*

$$Z(X + \widetilde{X}) = Z(X) + \sum_{k=0}^{r}\sum_{j=0}^{k} z_k \left(\widetilde{X^{p^j}}\right)^{p^{k-j}}$$

(where by convention $z_r = 1$).

Proof. This is a straightforward consequence of Proposition A.3.10. □

Corollary A.3.12. *Let $Z(T) = T^{p^r} + z_{r-1}T^{p^{r-1}} + \ldots z_1T^p + z_0T$ be any linearised polynomial with coefficients in R. Then in $Sym(A)\#A$ it holds*

$$Z\left(X + \widetilde{1}\right) = Z(X) + \sum_{k=0}^{r}\sum_{j=0}^{k} z_k \left(\widetilde{X^{p^j-1}}\right)^{p^{k-j}}$$

(where by convention $z_r = 1$).

Proof. Consider the morphism of R-algebras

$$\begin{aligned} \psi\colon R\left[\widetilde{X^i}\right]_{i\geq 0}\#R[X] &\to R\left[\widetilde{X^i}\right]_{i\geq 0}\#R[X] \\ \widetilde{X^i} &\mapsto \widetilde{X^{i+1}}, \\ X &\mapsto X. \end{aligned}$$

Notice that ψ is injective. Moreover,

$$\begin{aligned} \psi\left(Z\left(X + \widetilde{1}\right)\right) = Z\left(X + \widetilde{X}\right) &= Z(X) + \sum_{k=0}^{r}\sum_{j=0}^{k} z_k \left(\widetilde{X^{p^j}}\right)^{p^{k-j}} \\ &= \psi\left(Z(X) + \sum_{k=0}^{r}\sum_{j=0}^{k} z_k \left(\widetilde{X^{p^j-1}}\right)^{p^{k-j}}\right) \end{aligned}$$

and thus, by injectivity,

$$Z\left(X + \widetilde{1}\right) = Z(X) + \sum_{k=0}^{r}\sum_{j=0}^{k} z_k \left(\widetilde{X^{p^j-1}}\right)^{p^{k-j}}.$$

□

Corollary A.3.13. *Let* $Z(T) = T^{p^r} + z_{r-1}T^{p^{r-1}} + \dots z_1T^p + z_0T$ *be any linearised polynomial with coefficients in* R *and* B *be an* R*-algebra which is an* $R[X]$*-module algebra via* $v\colon R[X] \to \mathrm{End}_R(B)$*, that is* $v(X) = \partial\colon B \to B$ *is a derivation. Then in the ring of Ore polynomials* $B[X;\partial]$*and for any* $f \in B$ *it holds*

$$Z\left(X+f\right) = Z(X) + \sum_{k=0}^{r}\sum_{j=0}^{k} z_k \left(\partial^{p^j-1}(f)\right)^{p^{k-j}}$$

(where by convention $z_r = 1$*).*

Proof. By Corollary A.3.4

$$\varphi_f \otimes id\colon R\left[\widetilde{X^i}\right]_{i\geq 0} \#R[X] \to B\#R[X] = B[X;\partial]$$

is a morphism of algebras. Therefore

$$Z\left(X+f\right) = Z\left(\varphi_f \otimes id\left(X+\widetilde{1}\right)\right) = \varphi_f \otimes id\left(Z\left(X+\widetilde{1}\right)\right) =$$

$$\varphi_f \otimes id\left(Z(X) + \sum_{k=0}^{r}\sum_{j=0}^{k} z_k \left(\widetilde{X^{p^j-1}}\right)^{p^{k-j}}\right) = Z(X) + \sum_{k=0}^{r}\sum_{j=0}^{k} z_k \left(\partial^{p^j-1}(f)\right)^{p^{k-j}}$$

□

Notice that for example applying the result to the linearised polynomial $Z(T) = T^p$ we obtain that for any $f \in B$ it holds

$$(X+f)^p = X^p + \partial^{p-1}(f) + f^p$$

in the ring of Ore polynomials $B[X;\partial]$, which is a result that we will re-obtain also in the last section of this appendix.

Corollary A.3.14. *Let* $Z(T) = T^{p^r} + z_{r-1}T^{p^{r-1}} + \dots z_1T^p + z_0T$ *be any linearised polynomial with coefficients in* R*. Then in* $Sym(A)\#A$ *for all* $i \geq 0$ *it holds*

$$Z\left(X+\widetilde{X^i}\right) = Z(X) + \sum_{k=0}^{r}\sum_{j=0}^{k} z_k \left(\widetilde{X^{p^j-1+i}}\right)^{p^{k-j}}$$

(where by convention $z_r = 1$*).*

A.4 Reduced norm of a monic polynomial of degree 1 in the ring of Ore polynomials $K[X;\partial]$ with $\partial^p = 0$

The setting will be the following. Let k be a field of characteristic p, K be a k-algebra which is also a field and

$$\begin{aligned} v\colon k[X] &\to \mathrm{End}_k(K) \\ X &\mapsto \partial \end{aligned}$$

inducing a $k[X]$-module algebra structure on K, where $\Delta(X) = X \otimes 1 + 1 \otimes X$, so ∂ is a k-linear derivation on K. Denote $F = \{x \in K \mid \partial(x) = 0\}$ and suppose that $\varphi(\partial) = 0$ for some linearised polynomial $\varphi \in k[X]_{lin}$, so we actually have that $v\colon k[X]/(\varphi) \to \mathrm{End}_F(K)$ and $k[X]/(\varphi)$ is a Hopf algebra. Therefore, the module algebra structure corresponds to a comodule algebra structure

$$\rho\colon K \to K \otimes_k (k[X]/(\varphi))^\vee$$

and we require that this makes K into a $(k[X]/(\varphi))^\vee$-Galois object over F, that is $\mathrm{Spec}(K)$ is a torsor under the action of some finite k-group scheme. Recall that $k[X; Frob] \simeq k[X]_{lin}$ (see Example 1.1.28). We denote by $Ann(\partial)$ the non-zero polynomial in $k[X; Frob]$ corresponding to φ. We then have that $K[X; \partial]$ is an Azumaya algebra over its center $F[\varphi(X)]$ and thus we have a well-defined reduced norm on it.

The goal of this section is to prove the following result. We will give two proofs of it, the first one more direct using tools of combinatorics, the second one more constructive.

Proposition A.4.1. *Consider the ring of Ore polynomials $K[X; \partial]$ where $\partial\colon K \to K$ is a derivation of order p. Then for any $f \in K$ we have*

$$N_{rd}(X - f) = X^p - (f^p + \partial^{p-1}(f)).$$

Combinatorial proof

We begin with two lemmas of combinatorics for which we wish to thank Francesco Viganò for the key ideas.

Lemma A.4.2. *Let N be a positive integer and $(\lambda_1, \dots, \lambda_k)$ be a partition of N, that is a list of positive integers such that*

$$\lambda_1 + \cdots + \lambda_k = N,$$

then

$$\sum_{\sigma \in S_k} \binom{\lambda_{\sigma(1)} + \lambda_{\sigma(2)} - 1}{\lambda_{\sigma(1)}} \binom{\lambda_{\sigma(1)} + \lambda_{\sigma(2)} + \lambda_{\sigma(3)} - 1}{\lambda_{\sigma(1)} + \lambda_{\sigma(2)}} \cdots \binom{N-1}{\lambda_{\sigma(1)} + \cdots + \lambda_{\sigma(k-1)}}$$

$$= \binom{N}{\lambda_1, \dots, \lambda_k}$$

where the multinomial $\binom{N}{\lambda_1, \dots, \lambda_k}$ counts the number of ways of arranging N elements $\{1, \dots, N\}$ in exactly k subsets $\Gamma_1, \dots, \Gamma_k$ of cardinality respectively $\lambda_1, \dots, \lambda_k$.

Proof. Suppose that N is in Γ_k, then we can choose in

$$\binom{N-1}{\lambda_k - 1} = \binom{N-1}{\lambda_1 + \cdots + \lambda_{k-1}}$$

ways the remaining $\lambda_k - 1$ elements of Γ_k from the remaining $N-1$ elements. Now set

$$M := \max\{i \in \{1,\dots,N\} \mid i \notin \Gamma_k\}$$

and suppose that $M \in \Gamma_{k-1}$, then we can choose in

$$\binom{N-\lambda_k-1}{\lambda_{k-1}-1} = \binom{\lambda_1+\cdots+\lambda_{k-1}-1}{\lambda_1+\cdots+\lambda_{k-2}}$$

ways the remaining $\lambda_{k-1}-1$ elements of Γ_{k-1} from the remaining $N-\lambda_k-1$ elements. Iterating the reasoning we obtain

$$\binom{N-(\lambda_2+\cdots+\lambda_k)-1}{\lambda_1-1}\cdots\binom{N-\lambda_k-1}{\lambda_{k-1}-1}\binom{N-1}{\lambda_k-1} =$$

$$\binom{\lambda_1-1}{0}\binom{\lambda_1+\lambda_2-1}{\lambda_1}\binom{\lambda_1+\lambda_2+\lambda_3-1}{\lambda_1+\lambda_2}\cdots\binom{N-1}{\lambda_1+\cdots+\lambda_{k-1}}$$

arrangements. In order to obtain all of them we have to consider all the possible permutations of the indices $1,\dots,k$ that is

$$\binom{N}{\lambda_1,\dots,\lambda_k} =$$

$$\sum_{\sigma\in S_k}\binom{\lambda_{\sigma(1)}+\lambda_{\sigma(2)}-1}{\lambda_{\sigma(1)}}\binom{\lambda_{\sigma(1)}+\lambda_{\sigma(2)}+\lambda_{\sigma(3)}-1}{\lambda_{\sigma(1)}+\lambda_{\sigma(2)}}\cdots\binom{N-1}{\lambda_{\sigma(1)}+\cdots+\lambda_{\sigma(k-1)}}$$

as stated. □

Lemma A.4.3. *Consider the matrix with coefficients in a ring of positive characteristic p defined as follows:*

$$A_{ij} = \begin{cases} \binom{j}{i}a_{j-i} & i \le j \\ 1 & i = j+1 \\ 0 & i > j+1 \end{cases}$$

for $i,j = 0,\dots,p-1$. Then, $\det(A) = a_0^p + a_{p-1}$.

Proof. By definition,

$$\det(A) = \sum_{\sigma\in S_p}\operatorname{sgn}(\sigma)\prod_{j=0}^{p-1}A_{\sigma(j)j}.$$

Now, since $A_{ij} = 0$ for $i > j+1$, it suffices to reduce the above summation to the subset

$$T = \{\sigma \in S_p \mid \sigma(j) \le j+1 \quad \forall j = 0,\dots,p-1\} \subseteq S_p.$$

Notice that all the permutations in T, when written as products of disjoint cycles, have as factors cycles made of consecutive numbers (for example for $p=7$ we can have the permutation $(0)(123)(4)(56)$). Moreover T has cardinality 2^{p-1}: for example for $p=3$ it

holds $T = \{(012), (01), (12), e\}$ while (021) and (02) do not belong to T since 0 cannot have 2 as image. Now every permutation determines a monomial in the a_i's in $\det(A)$ and we wish to study the coefficients of such monomials. For example the identity determines the monomial a_0^p and the p-cycle $(012\cdots p)$ determines the monomial a_{p-1} (and moreover these monomials are not determined by any other permutation of the fixed subset). So actually we would like to show that the coefficients of all the other monomials appearing in the polynomial $\det(A)$ are zero.

Thanks to the nice form assumed by the permutations in T we can always write their cyclic decomposition with the numbers in order, with 0 being the first appearing and $p-1$ the last. Now, let us fix a permutation λ which is neither the p-cycle in T nor the identity, let k be the number of disjoint cycles composing λ and $(\lambda_1, \ldots, \lambda_k)$ be the k-tuple of lengths of the disjoint cycles of λ (for example for $\lambda = (0)(123)(4)(56)$ we have $k = 4$ and $(\lambda_1, \ldots, \lambda_4) = (1, 3, 1, 2)$). We can see that the monomial determined by λ is

$$\prod_{s=1}^{k} a_{\lambda_s - 1} = \prod_{i=1}^{p} a_{i-1}^{m_i}$$

where m_i is the number of cycles of length i appearing in λ. We therefore notice that permutations having the same number of cycles of a certain length determine the same monomial. Moreover these permutations have all the same sign. One also sees that the coefficient of the monomial determined by λ is

$$\binom{\lambda_1 - 1}{0}\binom{\lambda_1 + \lambda_2 - 1}{\lambda_1}\binom{\lambda_1 + \lambda_2 + \lambda_3 - 1}{\lambda_1 + \lambda_2}\cdots\binom{p-1}{\lambda_1 + \cdots + \lambda_{k-1}}.$$

The other coefficients are given by permutations having k-tuple $(\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(k)})$ for $\sigma \in S_k$, but we don't want to consider multiple times the same k-tuple, so they are in total $\frac{k!}{m_1! \ldots m_p!}$ (notice that we are never dividing by p since we assumed that λ is not the identity and thus $m_i < p$ for every i). All this tells us that the coefficient we are studying is exactly

$$\frac{1}{m_1! \ldots m_p!} \sum_{\sigma \in S_k} \binom{\lambda_{\sigma(1)} + \lambda_{\sigma(2)} - 1}{\lambda_{\sigma(1)}} \cdots \binom{p-1}{\lambda_{\sigma(1)} + \cdots + \lambda_{\sigma(k-1)}} =$$

$$\frac{1}{m_1! \ldots m_p!} \binom{p}{\lambda_1, \ldots, \lambda_k} = 0$$

where the first equality holds by Lemma A.4.2 □

We are now ready to give a proof of Proposition A.4.1.

Proof of Proposition A.4.1. We recall that we wish to show that for the ring of Ore polynomials $K[X; \partial]$ where $\partial \colon K \to K$ is a derivation of order p, it holds that for any $f \in K$

$$N_{rd}(X - f) = X^p - (f^p + \partial^{p-1}(f)).$$

By Lemma A.2.13 it holds

$$N_{rd}(X - f) = \det(r_{(X-f)})$$

where $r_{(X-f)}\colon K[X;\partial] \to K[X;\partial]$ is the $K[X^p]$-linear endomorphism of multiplication on the right by $X-f$ in the ring of Ore polynomials $K[X;\partial]$. We fix the basis $\{1, X, \dots, X^{p-1}\}$ for the free $K[X^p]$-module $K[X;\partial]$ and we obtain that the matrix corresponding to $r_{(X-f)}$ is

$$A_{ij} = \begin{cases} X^p - \partial^{p-1}(f) & (i,j) = (0, p-1) \\ -\binom{j}{i}\partial^{j-i}(f) & i \leq j, (i,j) \neq (0,p-1) \\ 1 & i = j+1 \\ 0 & i > j+1 \end{cases}$$

where $i, j = 0, \dots, p-1$. Then, by Lemma A.4.3 we deduce that $\det(r_{(X-f)}) = (-f)^p + X^p - \partial^{p-1}(f)$ and thus the claim is proved. □

Alternative proof

We start by recalling some results we need in the following, a reference for them is [Car18, Chapter 4].

Lemma A.4.4. *Let $\varphi\colon A \to B$ be a surjective homomorphism of rings. Then the image of the center of A lies in the center of B.*

Proof. Let $a \in Z(A)$ be a central element of A and take $b \in B$. Since φ is surjective $b = \varphi(\alpha)$ for some $\alpha \in A$. Therefore

$$\varphi(a)b = \varphi(a)\varphi(\alpha) = \varphi(a\alpha) = \varphi(\alpha a) = \varphi(\alpha)\varphi(a) = b\varphi(a)$$

that is $\varphi(a)$ lies in the center of B. □

Lemma A.4.5. *Consider the ring of Ore polynomials $K[X;\partial]$ where $\partial\colon K \to K$ is a non-zero derivation such that $Ann(\partial)$ has degree $m \geq 0$ and let $r = p^m$. Then for any $P \in K[X;\partial]$ it holds*

$$\deg(N_{rd}(P)) = r\deg(P).$$

Proof. See [Car18, Proposition 4.3.6]. □

Lemma A.4.6. *For any $P \in D = K[X;\partial]$ and $Q \in F[Ann_{lin}(X)] = Z(D)$ (the center of D) where $F = \{x \in K \mid \partial(x) = 0\}$ it holds that $RGCD(P,N) = 1$ if and only if $GCD(N_{rd}(P), Q) = 1$ (where RGCD denotes the right greatest common divisor).*

Proof. See [Car18, Lemme 4.3.8]. □

Lemma A.4.7. *For any irreducible polynomial $P \in D$ it holds that $N_{rd}(P)$ is, up to a constant, a power of an irreducible polynomial in $Z(D)$.*

Proof. See [Car18, Corollaire 4.3.9]. □

Proposition A.4.8. *Consider the ring of Ore polynomials $K[X;\partial]$ where $\partial\colon K \to K$ is a derivation of order p. Then for any $f \in K$ we have*

$$N_{rd}(X - f) = (X - f)^p.$$

Proof. Consider the isomorphism of rings

$$\begin{aligned} \psi\colon K[X;\partial] &\to K[X;\partial] \\ X &\mapsto X - f. \end{aligned}$$

We know that the center of the ring of Ore polynomials $K[X;\partial]$ is $F[X^p]$ where $F = \{x \in K \mid \partial(x) = 0\}$. Therefore, by Lemma A.4.4, since X^p is a central element, it holds that $\psi(X^p) = (X - f)^p$ is central as well. By Lemma A.4.5, $N_{rd}(X - f)$ has degree p. Moreover by Lemma A.4.6 we have, for $P \in K[X;\partial]$ and $N \in F[X^p]$, $RGDC(P, N) = 1$ if and only if $GCD(N_{rd}(P), N) = 1$ (where $RGCD$ denotes the right greatest common divisor). Choosing $P = X - f$ and $N = \psi(X^p) = (X - f)^p$ we obtain that

$$GCD(N_{rd}(X - f), \psi(X^p)) \neq 1.$$

By Lemma A.4.7, $N_{rd}(X - f)$ is irreducible, up to a constant, in $F[X^p]$. Moreover it is monic (see [Car18, Proposition 4.3.11]), therefore we have

$$GCD(N_{rd}(X - f), \psi(X^p)) = N_{rd}(X - f)$$

and since they both have degree p it holds $N_{rd}(X - f) = \psi(X^p) = (X - f)^p$. □

A reference for the following results that we need in order to give the alternative proof of Proposition A.4.1 can be found in [Put95], for convenience we also report here their proofs. I am thankful to Raphaël Pagès for pointing out this reference to me and for the helpful discussions we had.

Let K be a field of characteristic p and $\partial\colon K \to K$ be a derivation of order p. We denote by $D = K[X;\partial]$ the ring of Ore polynomials. Let M be a D-module that has dimension 1 over K and let us denote by $\{e\}$ a basis of M over K. Then we have $Xe = be$ for some $b \in K$. We define $\tau(b)$ by $X^p e = \tau(b)e$ (for example, for $p = 2$ we have $X^2 e = X(be) = (\partial(b) + bX)e = (\partial(b) + b^2)e$ that is $\tau(b) = \partial(b) + b^2$). Notice that

$$X^{p+1}e = X^p(be) = bX^p e = b\tau(b)e$$

but also

$$X^{p+1}e = X(\tau(b)e) = (\partial(\tau(b)) + \tau(b)b)e$$

from which we deduce that $\tau(b) \in F = \{x \in K \mid \partial(x) = 0\}$. We can define $\tau(b)$ for every $b \in K$ in the following way:

$$\begin{array}{rccccc} \tau\colon & K & \to & \{D - mod \text{ of } \dim_K = 1 \text{ with a base}\} & \to & K^p \\ & b & \mapsto & (Ke, Xe = be) & \mapsto & \text{coefficient of } X^p e \end{array}$$

Lemma A.4.9. *The map* $\tau\colon K \to K^p$ *is additive.*

Proof. Let Ke_i be D-modules of dimension 1 over K such that $Xe_i = b_i e_i$ for $i = 1, 2$. Then also $Ke_1 \otimes_K Ke_2$ is a D-module of dimension 1 over K with the action $X(m \otimes n) = X(m) \otimes n + m \otimes X(n)$. Therefore

$$X(e_1 \otimes e_2) = (b_1 + b_2)e_1 \otimes e_2.$$

Moreover

$$\tau(b_1 + b_2)e_1 \otimes e_2 = X^p(e_1 \otimes e_2) = X^p(e_1) \otimes e_2 + e_1 \otimes X^p(e_2) = (\tau(b_1) + \tau(b_2))e_1 \otimes e_2,$$

hence the claimed linearity. □

Lemma A.4.10. *Let* K *have the structure of* D*-module given by* $X(1) = b$*, then*

$$X^n(y) = (\partial + b\mathrm{id}_K)^n(y)$$

for every $y \in K$ *and* $n \geq 0$*. In particular* $(\partial + b\mathrm{id}_K)^p$ *is* K*-linear and*

$$\tau(b) = (\partial + b\mathrm{id}_K)^p(1).$$

Proof. Let us argue by induction on n. One sees that the equality holds for example for $n = 0, 1, 2$. Now let us suppose it holds true for n and show that then it is true for $n + 1$. Let $c = (\partial + b\mathrm{id}_K)^n(y) = X^n(y)$, then

$$X^{n+1}(y) = X(c) = (\partial(c) + cX)(1) = \partial(c) + cb = (\partial + b\mathrm{id}_K)(c) = (\partial + b\mathrm{id}_K)^{n+1}(y),$$

as wished. □

Proposition A.4.11. *In the ring of Ore polynomials* $K[X; \partial]$ *with* ∂ *a derivation of order* p*, it holds*

$$(X - b)^p = X^p - \tau(b)$$

for every $b \in K$*.*

Proof. Let

$$\begin{aligned} D &\to \mathrm{End}(K) \\ X &\mapsto (1 \mapsto b) \end{aligned}$$

be a structure of D-module on K. This induces

$$\begin{aligned} F[X^p] &\to \mathrm{End}(K) \\ X^p &\mapsto (1 \mapsto \tau(b)) \end{aligned}$$

whose kernel is the ideal $(X^p - \tau(b))$. Moreover, as seen in Proposition A.4.8, $(X - b)^p$ is an element of $F[X^p]$ and lies in the kernel as well. Now, since both polynomials are monic and share the same degree they must be equal (notice that $F[X^p]$ is a unique factorization domain). □

Alternative proof of Proposition A.4.1. By assumption ∂ is a derivation of order p, hence $[K : K^\partial] = p$ and thus $K = K^\partial(t)$ for any $t \in K \backslash K^\partial$. Moreover, by Proposition A.4.8 and A.4.11 we have

$$N_{rd}(X - b) = (X - b)^p = X^p - \tau(b)$$

and thus, since τ is additive, it is enough to show the result for $b = ct^i$ for $c \in K^\partial$ and $i = 0, \dots, p-1$. Now

$$(X - ct^i)^p = X^p - c^p t^{pi} - c^{p-1} f_{p-1,i}(t) - \cdots - c^2 f_{2,i}(t) - c f_{1,i}(t)$$

where the $f_{j,i}(t)$ are some polynomials in t over K^∂. Now, since $c \mapsto \tau(ct^i)$ is additive, the only polynomial that can occur is $f_{1,i}$. This summand appears in

$$(X - ct^i)^p = (X - ct^i)(X - ct^i) \dots (X - ct^i)(X - ct^i)$$

computing $X^{p-1} ct^i = cX^{p-1} t^i$ and one sees that the constant term of this polynomial in X is $c\partial^{p-1}(t^i)$. The claim is thus proved. □

Corollary A.4.12 (Jacobson identity)**.** *For every $b \in K$ it holds*

$$\tau(b) = \partial^{p-1}(b) + b^p.$$

Proof. Putting altogether Propositions A.4.1, A.4.8 and A.4.11 we have

$$X^p - b^p - \partial^{p-1}(b) = N_{rd}(X - b) = (X - b)^p = X^p - \tau(b)$$

hence the statement. □

Proposition A.4.13. *Let $\partial \colon K \to K$ be any derivation on K a field of characteristic p. For any $f \in K$ it holds*

$$(\partial + f\mathrm{id}_K)^p = \partial^p + (f^p + \partial^{p-1}(f))\mathrm{id}_K.$$

Proof. We begin by noticing that

$$(\partial + f\mathrm{id}_K)^p = \partial^p + \sum_{i=0}^{p-1} Q_i(f, \partial(f), \dots, \partial^{p-1}(f))\partial^i$$

where the Q_i are some universal polynomials in $\mathbb{F}_p[X_0, \dots, X_{p-1}]$. We can thus show the result for ∂ such that $\partial^p = 0$. Now, by Lemma A.4.10 along with Corollary A.4.12, we have that $(\partial + f\mathrm{id}_K)^p$ is K-linear and

$$(\partial + f\mathrm{id}_K)^p(1) = f^p + \partial^{p-1}(f)$$

and the statement follows, since two K-linear endomorphisms of K with same image of 1 are the same. □

Example A.4.14. In the same context as above, that is the ring of Ore polynomials $K[X;\partial]$ with $\partial^p = 0$, let us compute $N_{rd}(fX)$ for $f \in K^\times$. By Lemma A.2.13 we have

$$N_{rd}(fX) = \det(r_{fX})$$

where r_{fX} is the multiplication on the right by fX on $K[X;\partial]$ over $K[X^p]$. We fix the basis $\{1, X, \ldots, X^{p-1}\}$. Then we have

$$X^j(fX) = \sum_{i=0}^{j} \binom{j}{i} \partial^{j-i}(f) X^{i+1}$$

for every $j = 0, \ldots, p-1$ that is the matrix associated to r_{fX} is

$$A = \begin{pmatrix} 0 & 0 & 0 & & fX^p \\ f & \partial f & \partial^2 f & & . \\ 0 & f & 2\partial f & & . \\ & & f & & \\ & & & . & . \\ & & & & f\,(p-1)\,\partial f \end{pmatrix}$$

or more precisely

$$A_{ij} = \begin{cases} fX^p & (i,j) = (0, p-1) \\ 0 & (i = 0, j < p-1) \text{ and for } i > j+1 \\ \binom{j}{i-1}\partial^{j-i+1}(f) & \text{for } 0 < i \leq j+1. \end{cases}$$

We then deduce that

$$N_{rd}(fX) = f^p X^p.$$

Proposition A.4.15. *Let $\partial\colon K \to K$ be any derivation on K a field of characteristic p. For any $f \in K$ it holds*

$$(f\partial)^p = f^p\partial^p - f\partial^{p-1}(f^{p-1})\partial = f^p\partial^p - f^{p+1}\partial^{p-1}\left(\frac{1}{f}\right)\partial.$$

Proof. We begin by noticing that

$$(f\partial)^p = f^p\partial^p + \sum_{i=0}^{p-1} Q_i(f, \partial(f), \ldots, \partial^{p-1}(f))\partial^i$$

where the Q_i are some universal polynomials in $\mathbb{F}_p[X_0, \ldots, X_{p-1}]$. In particular, we can thus deal with the case $\partial^p = 0$. Now, $(f\partial)^p$ is a derivation and thus the only Q_i that can occur is Q_1. Consider the evaluation morphism

$$\begin{aligned} K[X;\partial] &\to \mathrm{End}_{\mathbb{Z}}(K) \\ X &\mapsto \partial. \end{aligned}$$

We then have $(fX)^p = f^p X^p + Q_1 X$. Since 1 and fX commute, the Newton binomial formula holds and we have

$$(fX+1)^p = (fX)^p + 1 = f^p X^p + Q_1 X + 1.$$

Now, using Proposition A.4.1, we see that

$$N_{rd}(fX+1) = f^p N_{rd}\left(X + \frac{1}{f}\right) = f^p\left(X^p + \frac{1}{f^p} + \partial^{p-1}\left(\frac{1}{f}\right)\right) = f^p X^p + 1 + f^p \partial^{p-1}\left(\frac{1}{f}\right).$$

Moreover, $(fX+1)^p$ and $N_{rd}(fX+1)$ are both divisible by $(fX+1)$, which then divides the difference

$$(fX+1)^p - N_{rd}(fX+1) = Q_1 X - f^p \partial^{p-1}\left(\frac{1}{f}\right)$$

that is

$$Q_1 X - f^p \partial^{p-1}\left(\frac{1}{f}\right) = c(fX+1).$$

Comparing the coefficients we see that $c = -f^p \partial^{p-1}\left(\frac{1}{f}\right)$ and $Q_1 = cf = -f^{p+1}\partial^{p-1}\left(\frac{1}{f}\right)$. The result follows. □

Bibliography

[AG60] Maurice Auslander and Oscar Goldman. "The Brauer group of a commutative ring". In: *Trans. Amer. Math. Soc.* 97 (1960), pp. 367–409.

[BC23] Elena Berardini and Xavier Caruso. *Algebraic Geometry codes in the sum-rank metric*. 2023. arXiv: 2303.08903 [math.AG].

[Bea10] Arnaud Beauville. "Finite subgroups of $\mathrm{PGL}_2(K)$". In: *Vector bundles and complex geometry*. Vol. 522. Contemp. Math. Amer. Math. Soc., Providence, RI, 2010, pp. 23–29.

[Beg69] Lucile Begueri. "Schéma d'automorphisms. Application à l'étude d'extensions finies radicielles". In: *Bull. Sci. Math. (2)* 93 (1969), pp. 89–111.

[BF03] Grégory Berhuy and Giordano Favi. "Essential dimension: a functorial point of view (after A. Merkurjev)". In: *Doc. Math.* 8 (2003), pp. 279–330.

[BM11] Sylvain Brochard and Ariane Mézard. "About de Smit's question on flatness". In: *Math. Z.* 267.1-2 (2011), pp. 385–401.

[Bou90] N. Bourbaki. *Algebra. II. Chapters 4–7*. Elements of Mathematics (Berlin). Translated from the French by P. M. Cohn and J. Howie. Springer-Verlag, Berlin, 1990.

[BR97] J. Buhler and Z. Reichstein. "On the essential dimension of a finite group". In: *Compositio Math.* 106.2 (1997), pp. 159–179.

[Bri22] Michel Brion. *Actions of finite group schemes on curves*. 2022. arXiv: 2207.08209 [math.AG].

[Car18] Xavier Caruso. "Polynômes de Ore en une variable". Notes de cours. Jan. 2018.

[CD23] Xavier Caruso and Amaury Durand. "Duals of linearized Reed-Solomon codes". In: *Des. Codes Cryptogr.* 91.1 (2023), pp. 241–271.

[Cha72] Stephen U. Chase. "On the automorphism scheme of a purely inseparable field extension". In: *Ring theory (Proc. Conf., Park City, Utah, 1971)*. Academic Press, New York-London, 1972, pp. 75–106.

[CS69] S.U. Chase and M.E. Sweedler. *Hopf Algebras and Galois Theory*. Lecture Notes in Mathematics. Springer Berlin Heidelberg, 1969.

[Del78] Ph. Delsarte. “Bilinear forms over a finite field, with applications to coding theory”. In: *J. Combin. Theory Ser. A* 25.3 (1978), pp. 226–241.

[DG70] Michel Demazure and Pierre Gabriel. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs.* Avec un appendice *Corps de classes local* par Michiel Hazewinkel. Masson & Cie, Éditeurs, Paris and North-Holland Publishing Co., Amsterdam, 1970, pp. xxvi+700.

[DI71] Frank DeMeyer and Edward Ingraham. *Separable algebras over commutative rings.* Lecture Notes in Mathematics, Vol. 181. Springer-Verlag, Berlin-New York, 1971, pp. iv+157.

[Dol09] I. V. Dolgachev. “On elements of order p^s in the plane Cremona group over a field of characteristic p”. In: *Tr. Mat. Inst. Steklova* 264.Mnogomernaya Algebraicheskaya Geometriya (2009), pp. 55–62.

[Dol10] Igor V. Dolgachev. “Finite subgroups of the plane Cremona group”. In: *Algebraic geometry in East Asia—Seoul 2008*. Vol. 60. Adv. Stud. Pure Math. Math. Soc. Japan, Tokyo, 2010, pp. 1–49.

[EW67] Shizuo Endo and Yutaka Watanabe. “On separable algebras over a commutative ring”. In: *Osaka Math. J.* 4 (1967), pp. 233–242.

[Fak20] Najmuddin Fakhruddin. “Finite group schemes of essential dimension one”. In: *Doc. Math.* 25 (2020), pp. 55–64.

[Gab85] È. M. Gabidulin. “Theory of codes with maximum rank distance”. In: *Problemy Peredachi Informatsii* 21.1 (1985), pp. 3–16.

[GH69] Jens Gamst and Klaus Hoechsmann. “Quaternions généralisés”. In: *C. R. Acad. Sci. Paris Sér. A-B* 269 (1969), A560–A562.

[Gol61] Oscar Goldman. “Determinants in projective modules”. In: *Nagoya Math. J.* 18 (1961), pp. 27–36.

[Gop82] V. D. Goppa. “Algebraic-geometric codes”. In: *Izv. Akad. Nauk SSSR Ser. Mat.* 46.4 (1982), pp. 762–781, 896.

[Gou23] Bianca Gouthier. *Infinitesimal rational actions.* 2023. arXiv: `2312.01765 [math.AG]`.

[GS06] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology.* Vol. 101. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2006, pp. xii+343.

[GT24] Bianca Gouthier and Dajano Tossici. *Unexpected subgroup schemes of* $\mathrm{PGL}_{2,k}$ *in characteristic 2.* 2024. arXiv: `2403.09469 [math.AG]`.

[Kno95] Friedrich Knop. “Homogeneous varieties for semisimple groups of rank one”. In: *Compositio Math.* 98.1 (1995), pp. 77–89.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves.* Vol. 6. Oxford Graduate Texts in Mathematics. Translated from the French by Reinie Erné, Oxford Science Publications. Oxford University Press, Oxford, 2002.

[Mar18] Umberto Martínez-Peñas. "Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring". In: *J. Algebra* 504 (2018), pp. 587–612.

[Mil17] J. S. Milne. *Algebraic groups*. Vol. 170. Cambridge Studies in Advanced Mathematics. The theory of group schemes of finite type over a field. Cambridge University Press, Cambridge, 2017, pp. xvi+644.

[Mil80] James S. Milne. *Étale cohomology*. Vol. No. 33. Princeton Mathematical Series. Princeton University Press, Princeton, NJ, 1980, pp. xiii+323.

[MO67] Hideyuki Matsumura and Frans Oort. "Representability of group functors, and automorphisms of algebraic schemes". In: *Invent. Math.* 4 (1967), pp. 1–25.

[Mon93] Susan Montgomery. *Hopf algebras and their actions on rings*. Vol. 82. CBMS Regional Conference Series in Mathematics. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1993, pp. xiv+238.

[MSK22] Umberto Martínez-Peñas, Mohannad Shehadeh, and Frank R. Kschischang. "Codes in the sum-rank metric: fundamentals and applications". English. In: *Found. Trends Commun. Inf. Theory* 19.5 (2022), pp. 814–1031.

[Mum08] David Mumford. *Abelian varieties*. Vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008.

[NWW15] Van C. Nguyen, Linhong Wang, and Xingting Wang. "Classification of connected Hopf algebras of dimension p^3 I". In: *J. Algebra* 424 (2015), pp. 473–505.

[Oor66] F. Oort. *Commutative group schemes*. Springer-Verlag, Berlin-New York, 1966, vi+133 pp. (not consecutively paged).

[Oor75] Frans Oort. "Which abelian surfaces are products of elliptic curves?" In: *Math. Ann.* 214 (1975), pp. 35–47.

[Ore33] Oystein Ore. "Theory of non-commutative polynomials". In: *Ann. of Math. (2)* 34.3 (1933), pp. 480–508.

[Pin05] Richard Pink. *Finite group schemes*. Lecture course in WS 2004/05, ETH Zürich. 2005.

[Pri08] Rachel Pries. "A short guide to p-torsion of abelian varieties in characteristic p". In: *Computational arithmetic geometry*. Vol. 463. Contemp. Math. Amer. Math. Soc., Providence, RI, 2008, pp. 121–129.

[Put95] Marius van der Put. "Differential equations in characteristic p". In: vol. 97. 1-2. Special issue in honour of Frans Oort. 1995, pp. 227–251.

[RS60] I. S. Reed and G. Solomon. "Polynomial codes over certain finite fields". In: *J. Soc. Indust. Appl. Math.* 8 (1960), pp. 300–304.

[Sal80] David J. Saltman. "Norm polynomials and algebras". In: *J. Algebra* 62.2 (1980), pp. 333–345.

[SGA3] Michael Artin, Jean-Etienne Bertin, Michel Demazure, Alexander Grothendieck, Pierre Gabriel, Michel Raynaud, and Jean-Pierre Serre. *Schémas en groupes.* Séminaire de Géométrie Algébrique de l'Institut des Hautes Études Scientifiques. Paris: Institut des Hautes Études Scientifiques, 1963/1966.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves.* Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513.

[Smi68] T. H. M. Smits. "Nilpotent S-derivations". In: *Indag. Math.* 30 (1968). Nederl. Akad. Wetensch. Proc. Ser. A 71, pp. 72–86.

[Swe69] Moss E. Sweedler. *Hopf algebras.* W. A. Benjamin, Inc., New York, 1969.

[Tos19] Dajano Tossici. "Essential dimension of infinitesimal commutative unipotent group schemes". In: *Boll. Unione Mat. Ital.* 12.4 (2019), pp. 575–581.

[TV13] Dajano Tossici and Angelo Vistoli. "On the essential dimension of infinitesimal group schemes". In: *Amer. J. Math.* 135.1 (2013), pp. 103–114.