UNIVERSIDADE ESTADUAL DE CAMPINAS
Instituto de Matemática, Estatística e Computação Científica

YURI DA SILVA

Módulos de Dieudonné e grupos p–divisíveis

Campinas

2024

YURI DA SILVA

Módulos de Dieudonné e grupos p–divisíveis

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática.

Orientador: Saeed Tafazolian

ESTE TRABALHO CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELO ALUNO YURI DA SILVA, E ORIENTADA PELO PROF. DR. SAEED TAFAZOLIAN.

Campinas

2024

Ficha catalográfica
Universidade Estadual de Campinas (UNICAMP)
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

Si38m

Silva, Yuri da, 2001-
Módulos de Dieudonné e grupos p-divisíveis / Yuri da Silva. – Campinas, SP [s.n.], 2024.

Orientador(es): Saeed Tafazolian.
Dissertação (mestrado) – Universidade Estadual de Campinas (UNICAMP), Instituto de Matemática, Estatística e Computação Científica.

1. Esquemas de grupos (Matemática). 2. Anéis de Witt . 3. Módulo de Dieudonné. I. Tafazolian, Saeed, 1978-. II. Universidade Estadual de Campinas (UNICAMP). Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações complementares

Título em outro idioma: Dieudonné-modules and p-divisible groups
Palavras-chave em inglês:
Group schemes (Mathematics)
Witt rings
Dieudonné module
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Pietro Speziali
Ethan Guy Cotterill
Gilberto Brito de Almeida Filho
Data de defesa: 25-10-2024
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0009-0007-1609-6720
- Currículo Lattes do autor: https://lattes.cnpq.br/1344396537917842

Dissertação de Mestrado defendida em 25 de outubro de 2024 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof. Dr. PIETRO SPEZIALI

Prof. Dr. ETHAN GUY COTTERILL

Prof. Dr. GILBERTO BRITO DE ALMEIDA FILHO

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Agradeço ao orientador Saeed Tafazolian, ao Instituto de Matemática da Unicamp, e à minha família.

— Yuri da Silva, 2024

Resumo

Na geometria algébrica, estudam-se grupos em conjuntos de soluções (nalgum corpo) de equações polinomiais cujas operações também são dadas por polinômios; neste texto, limitaremos ao conceito de esquemas-grupos afins. O objetivo aqui será classificar os esquemas-grupos afins abelianos sobre um corpo perfeito, especificamente em característica $p > 0$, o caso mais difícil. Para tal, será dada a teoria da antiequivalência de Dieudonné, após o estudo de vetores de Witt. No final, menciona-se um pouco sobre esquemas-grupos p-divisíveis (ou de Barsotti–Tate), e suas relações com p–torções de variedades abelianas.

Palavras-chaves: esquema-grupo, vetor de Witt, módulo de Dieudonné, p-divisível

Abstract

In algebraic geometry are studied groups on sets of solutions (over a field) of polynomial equations whose operations are also given by polynomials; in this text we will limit to the concept of affine group-schemes. The objective here will be the classification of abelian affine group-schemes over a perfect field, specifically of characteristic $p > 0$, the most difficult case. For that, the theory of the Dieudonné-antiequivalence will be given, after the study of Witt-vectors. In the end, a bit is mentioned about p-divisible group-schemes (or Barsotti–Tate-groups), and their relations with p–torsions of abelian varieties.

Key-words: group-scheme, Witt-vetor, Dieudonné-module, p-divisible

Sumário

1 Introdução **10**
1.1 Notações 11

2 Básico da teoria das categorias **12**
2.1 A definição de categoria 12
2.1.1 Das fundações 13
2.2 Functores 13
2.3 Tipos de setas 14
2.4 Transformações naturais 14
2.4.1 Tipos de functores, equivalência 15
2.5 Lema de Yoneda 15
2.6 Limites e colimites 16
2.7 Adjunções 17
2.8 Objetos-grupos 18
2.9 Categorias abelianas 19
2.9.1 Ações em sequências exatas 23

3 Decomposição de álgebras **27**
3.1 Conjuntos algébricos 27
3.1.1 Espaços topológicos noetherianos 28
3.2 Álgebras separáveis 31
3.2.1 Maior subálgebra separável 33

4 Esquemas-grupos afins **36**
4.1 Esquemas afins 36
4.1.1 Comódulos 39
4.2 Alguns esquemas-grupos afins específicos 39
4.3 Dualidade de Cartier 41
4.3.1 Esquema de homomorfismos 42
4.4 Os fatores reduzido e conexo 43
4.5 Em direção à categoria abeliana dos esquemas-grupos afins abelianos algébricos 44

4.5.1 Álgebras de Hopf reduzidas . . . 44
4.5.2 Álgebras de Hopf com ideais maximais nilpotentes . . . 46
4.5.3 Fielmente planos . . . 46
4.5.4 Álgebras de Hopf fielmente planas . . . 48
4.5.5 Os quocientes . . . 50
4.5.6 Subgrupos fechados são núcleos . . . 51
4.5.7 A prova . . . 53
4.5.8 Multiplicatividade de ordens . . . 55

5 Mapas de Frobenius e Verschiebung **56**
5.1 Definição e propriedades básicas . . . 56
5.1.1 Relacionando-os com álgebras separáveis, conexas . . . 59

6 Vetores de Witt **60**
6.1 A definição dos vetores de Witt . . . 60
6.1.1 Relação com os p-ádicos . . . 63
6.1.2 Usando séries geradoras . . . 64
6.1.3 Frobenius e Verschiebung nos vetores de Witt . . . 65
6.1.4 Os ideais de $W(k)$ . . . 66
6.2 Pareamento de vetores de Witt . . . 67
6.2.1 Esquemas formais . . . 69
6.2.2 Duais de W_n^m, W_n, e W . . . 71
6.3 Anel de Dieudonné . . . 74
6.4 Em direção ao teorema de classificação . . . 76
6.4.1 Extensões por W_1 . . . 78
6.4.2 A prova . . . 81
6.4.3 Relação com duais . . . 85

7 Os esquemas-grupos p-divisíveis **88**
7.1 O básico . . . 88
7.2 Módulos de Cartier . . . 89
7.3 Uso com torções de variedades abelianas . . . 92

Bibliografia **93**

Capítulo 1

Introdução

Este texto tem o objetivo de dar os fundamentos da "antiequivalência de Dieudonné", na geometria algébrica. O pré-requisito é apenas a mais básica teoria dos anéis comutativos.

O capítulo 1 tem uma breve introdução ao mínimo da teoria das categorias. Explicações mais completas e mais exemplos estão nas referências citadas.

O capítulo 2 tem o início da geometria algébrica, que é o estudo da geometria das soluções de equações polinomiais; porém aqui só se trata de quando esses conjuntos de soluções formam um grupo. Também tem resultados sobre decomposições de k-álgebras como certos produtos ou produtos tensoriais.

O capítulo 3 é sobre esquemas-afins F, em que cada $F(A)$, para k-álgebras A, é o conjunto de soluções em A^I dum mesmo sistema de equações polinomiais (independente de A), sem exigir I finito. Por teoria de categorias, será o mesmo que uma única álgebra B, dita "álgebra representante", dada por geradores $(x_i)_{i\in I}$ e relações $f(x_i)_{i\in I} = 0$ para cada f no sistema de equações. Mas aqui só se estuda quando F tem operações de grupos, que será o mesmo que B ter "operações de cogrupo", ou ser uma "álgebra de Hopf". Veremos o "dual de Cartier", a troca das operações de álgebra com as operações de cogrupo, e vice-versa. E ao longo de muitas páginas, incluindo um estudo de módulos (fielmente) planos, tento dar a prova completa de que essas álgebras de Hopf formam uma "categoria abeliana", para poderem ser manipuladas, sem muita dificuldade, como se fossem módulos.

O capítulo 4 trata da operação "Frobenius" F em álgebras de Hopf, que não é muito mais do que potências $a \mapsto a^p$, usada para estudar os nilpotentes, e uma operação "dual", o "Verschiebung" V.

O capítulo 5 tem como objetivo a antiequivalência de Dieudonné. Inicia com os "vetores de Witt", antes usados para estudar extensões cíclicas de corpos, mas aqui importantes por terem operação peculiar em vetores $(x_0, x_1, \ldots) \in W(A \in k\text{−}\mathsf{Alg})$, $k \supseteq \mathbb{F}_p$, satisfazendo $(x_0, x_1, \ldots) = (x_0, 0^\infty) + (0, x_1, 0^\infty) + \cdots$, e $p \cdot (x_0, x_1, \ldots) = (0, x_0^p, x_1^p, \ldots)$. A multiplicação e um "exponencial" serão usados num "pareamento" $W \times \widehat{W} \to$

$\boldsymbol{G_m}$, que será usado para calcular duais de Cartier. E ao longo de muitas páginas, incluindo um estudo de extensões $0 \to W_n \to (\cdots) \to (\cdots) \to 0$, tento dar a prova completa de que o "functor de Dieudonné" forma uma antiequivalência duma certa subcategoria de esquemas-grupos afins abelianos a certa subcategoria de módulos sobre o "anel de Dieudonné" $E = \cdots \oplus W(k) \cdot V \oplus W(k) \oplus W(k) \cdot F \oplus W(k) \cdot F^2 \oplus \cdots$; depois são dadas variantes dessa antiequivalência.

E o capítulo 6 é sobre os "p-divisíveis", que são certas "torres" $G_0 \to G_1 \to \cdots$, que terão uma outra antiequivalência com "torres inversas" $M_0 \leftarrow M_1 \leftarrow \cdots$ de módulos de Dieudonné. Brevemente se diz sobre "módulos de Cartier" e como num certo caso são isomorfos aos de Dieudonné; e depois, sem provas, como essa teoria toda poderia ser usada com as "p-torções" de "variedades abelianas" em característica p, tais como as curvas elípticas e outros grupos definidos nos espaços projetivos.

Espero que este texto possa ser útil para clarificar as provas dos fatos da teoria da antiequivalência de Dieudonné, sem depender de teorias mais complicadas.

1.1 Notações

Letras: E anel de Dieudonné. F mapa de Frobenius. f Frobenius $W^{m+1} \to W^m$. $\boldsymbol{G_a}$ esquema afim $R \mapsto (R, +)$. $\boldsymbol{G_m}$ esquema afim $R \mapsto (R^\times, \cdot)$. $\underline{\mathrm{Hom}}$ esquema de homomorfismos. $I(\_)$ ideal dos polinômios anulando-se. S coinverso (Hopf). V mapa Verschiebung. v Verschiebung $W_n \to W_{n+1}$. $W, W_n, W_n^m, W^m, \widehat{W}, \widehat{W}^m$ vetores de Witt. $Z(\_)$ fechado algébrico, de espectro. $\underline{\alpha}_{p^n}$ esquema afim $R \mapsto (\{x \in R \mid x^{p^n} = 0\}, +)$. Δ comultiplicação (Hopf). ϵ counidade (Hopf). $\underline{\mu}_n$ esquema afim $R \mapsto (\{x \in R \mid x^n = 1\}, \cdot)$. π_0 maior subálgebra separável.

Símbolos: A_K extensão de escalares. $\overline{k}$ fecho algébrico. k_s maior k-corpo separável. $\mathcal{A}^\circ$ categoria oposta. $a_{\bullet\bullet}$ matriz de componentes $a_{i,j}$. $|G|$ ordem (dimensão de álgebra associada); valor absoluto. $\times_H$ produto fibrado $\cdots \to H \leftarrow \cdots$. $R^\times$ grupo dos inversíveis. $k[S]$ álgebra associada a fechado algébrico; álgebra de monoide. $[x]$ classe de equivalência. $[a \lessgtr b]$ vale 1 se $a \lessgtr b$, vale 0 caso contrário. A^* espaço vetorial dual, dual de Cartier. $\triangledown$ prova continua. $\sqcup$ coproduto, mínimo múltiplo comum. $\sqcap$ máximo divisor comum. $\hookrightarrow$ mônico. $\twoheadrightarrow$ épico. (f, g) dupla, seta ao produto. $\langle f, g \rangle$ seta do coproduto (em particular, para morfismos de álgebras, $\langle f, g \rangle (a \otimes b) = fa \cdot gb$); pareamento de vetores de Witt. $\langle \cdots \rangle_A$ A-submódulo (ou ideal) gerado. $\sqsubseteq$ divisor.

Capítulo 2

Básico da teoria das categorias

A teoria das categorias é ampla, e aqui consideramos somente suas partes mais básicas, que, mesmo quase triviais, são muito úteis para formulações e demonstrações breves e eficientes.

Para aprofundar-se: (Riehl, 2016), (Mac Lane, 1998).

2.1 A definição de categoria

Definição 2.1.1. Uma "categoria" consiste duma classe $O_{\mathcal{C}}$ e de conjuntos $\mathcal{C}(A, B)$ para quaisquer $A, B \in O_{\mathcal{C}}$, e também de operações $1_A \in \mathcal{C}(A, A)$, $(\circ) = (\circ_{A,B,C}) \in \mathcal{C}(B, C) \times \mathcal{C}(A, B) \to \mathcal{C}(A, C)$ (para cada $A, B, C \in O_{\mathcal{C}}$) satisfazendo (para quaisquer $A, B, C, D \in O_{\mathcal{C}}$):

- (elemento neutro) $\forall_{f \in \mathcal{C}(A,B)} f \circ 1_A = f$ e $\forall_{g \in \mathcal{C}(C,A)} 1_A \circ g = g$;
- (associatividade) $\forall_{f \in \mathcal{C}(A,B)} \forall_{g \in \mathcal{C}(B,C)} \forall_{h \in \mathcal{C}(C,D)} (h \circ g) \circ f = h \circ (g \circ f)$.

Os elementos de $O_{\mathcal{C}}$ são chamados "objetos", e os elementos de $\mathcal{C}(A, B)$ (ou $\hom_{\mathcal{C}}(A, B)$) são chamados de "setas" (ou morfismos) do domínio A ao contradomínio B.

Exemplo 2.1.2. Há categoria Conj cujos objetos são os conjuntos, e tais que $\mathsf{Conj}(A, B)$ consiste de todas as funções $A \to B$. As operações $(\circ) = (\circ_{A,B,C})$ são dadas pela composição de funções, enquanto que as 1_A são as funções-identidades.

Exemplo 2.1.3. Para cada anel comutativo unitário R, há a categoria $R{-}\mathsf{Alg}$ cujos objetos são as R-álgebras, e tais que $R{-}\mathsf{Alg}(A, B)$ consiste de todos os homomorfismos de R-álgebras $A \to B$. As operações $\circ$ e 1_A são as mesmas que em Conj.

Similarmente há a categoria Grp dos grupos, a Ab dos grupos abelianos, a Top dos espaços topológicos, etc.

Exemplo 2.1.4. Cada conjunto X com uma pré-ordem $\leq$ (isto é, uma relação reflexiva e transitiva) pode ser considerado uma categoria, cujos objetos são precisamente os

elementos de X, e com conjuntos de setas $X(a,b) \coloneqq \{\bullet \mid a \leq b\}$, isto é, $X(a,b)$ é vazio se $a \not\leq b$ e $X(a,b)$ tem precisamente um elemento quando $a \leq b$. As operações $\circ$ podem ser definidas pela transitividade de $\leq$, enquanto que as 1 usam a reflexividade de $\leq$.

Exemplo 2.1.5. Dada categoria $\mathcal{A}$, denota-se por $\mathcal{A}^\circ$ (a categoria "oposta") a categoria cujos objetos são os mesmos que os de $\mathcal{A}$, mas com $\mathcal{A}^\circ(A,B) \coloneqq \mathcal{A}(B,A)$; assim a operação $\circ$ em $\mathcal{A}^\circ$ é "oposta": $f \circ^{\mathcal{A}^\circ} g \coloneqq g \circ^{\mathcal{A}} f$.

Dada outra categoria $\mathcal{B}$, denota-se por $\mathcal{A} \times \mathcal{B}$ (a "categoria-produto") a cujos objetos são duplas $(A \in O_{\mathcal{A}}, B \in O_{\mathcal{B}})$, e com $(\mathcal{A} \times \mathcal{B})((A,B),(A',B')) \coloneqq \mathcal{A}(A, A') \times \mathcal{B}(B,B')$, com $1_{(A,B)} \coloneqq (1_A, 1_B)$ e $(f',g') \circ (f,g) \coloneqq (f' \circ f, g' \circ g)$.

2.1.1 Das fundações

Para fugir de paradoxos lógicos, quando dizemos "categoria dos conjuntos", "categoria dos anéis", etc., implicitamente entendemos como categoria de conjuntos, anéis, etc., dentro dum certo universo $\mathcal{U}$. Por exemplo, $\mathcal{U}$ pode ser a família dos anéis de elementos dentro de $k \times k \times \cdots$, k corpo, com operações quaisquer. As propriedades dessas categorias podem variar dependendo de $\mathcal{U}$, mas não se terá muito rigor em dizer quais hipóteses sobre $\mathcal{U}$ serão usadas. (Por exemplo, $\mathcal{U}$ pode ser um ϵ-modelo duma teoria de conjuntos mais fraca). Uma "categoria pequena" será uma categoria que seja elemento de $\mathcal{U}$.

2.2 Functores

Se um homomorfismo de grupos preserva a operação de grupos (e o elemento neutro e a operação de inverso), um "homomorfismo de categorias" deve preservar as identidades e composições:

Definição 2.2.1. Dadas categorias $\mathcal{A}$ e $\mathcal{B}$, um "functor" $F : \mathcal{A} \to \mathcal{B}$ consiste duma função $O_F : O_{\mathcal{A}} \to O_{\mathcal{B}}$ e de funções $F_{A,B} : \mathcal{A}(A,B) \to \mathcal{B}(O_F A, O_F B)$ satisfazendo (para quaisquer $A, B, C \in O_{\mathcal{A}}$):

- (identidade) $F_{A,A}(1_A) = 1_{O_F A}$;
- (composição) $\forall_{f \in \mathcal{A}(B,C)} \forall_{g \in \mathcal{A}(A,B)} F_{A,C}(f \circ g) = F_{B,C}(f) \circ F_{A,B}(g)$.

Exemplo 2.2.2. Dada categoria $\mathcal{A}$, dado objeto fixo $X \in O_{\mathcal{A}}$, há o functor $\hom(X, \_) : \mathcal{A} \to \mathsf{Conj}$, dado por: $O_{\hom(X,)}(A \in O_{\mathcal{A}}) \coloneqq \mathcal{A}(X,A)$, e $(\hom(X,\_))_{A,B}(f \in \mathcal{A}(A, B)) \coloneqq (p \in O_{\hom(X,)}(A)) \mapsto (f \circ p \in O_{\hom(X,)}(B))$. (Chama-se "functor hom covariante").

Exemplo 2.2.3. Assim como no exemplo anterior, há functor $\hom(\_, X) : \mathcal{A}^\circ \to \mathsf{Conj}$ (cujo domínio é $\mathcal{A}^\circ$ não $\mathcal{A}$). (Chama-se "functor hom contravariante").

No caso particular em que $\mathcal{A}$ é a categoria dos R-módulos $R{-}\mathsf{Mod}$, e em que $X \coloneqq R$, obtém-se precisamente o functor dos duais: $O_{\hom(,R)}(M) = M^*$.

Exemplo 2.2.4. Se $\mathcal{A}$ é uma categoria finita, como o "quadrado" $\begin{array}{ccc} 0 & \to & 1 \\ \downarrow & \searrow & \downarrow \\ 2 & \to & 3 \end{array}$, um functor $F : \mathcal{A} \to \mathcal{B}$ é o mesmo que um "diagrama comutativo", como $\begin{array}{ccc} F0 & \to & F1 \\ \downarrow & \searrow & \downarrow \\ F2 & \to & F3 \end{array}$.

2.3 Tipos de setas

Definição 2.3.1. Uma seta $f : A \to B$ numa categoria $\mathcal{C}$ é dita ser:

- um "monomorfismo" (ou mônica) sse $\forall_{x,y:(\cdots)\to A} f \circ x = f \circ y \implies x = y$;
- um "epimorfismo" (ou épica) sse $\forall_{p,q:B\to(\cdots)} p \circ f = q \circ f \implies p = q$;
- uma "seção" (ou inversa direita) sse $\exists_{r:B\to A} r \circ f = 1_A$;
- uma "retração" (ou inversa esquerda) sse $\exists_{s:B\to A} f \circ s = 1_B$;
- um "isomorfismo" sse $\exists!_{g:B\to A} g \circ f = 1_A \wedge f \circ g = 1_B$ (escreve-se $f^{-1} \coloneqq g$).

(Temos seção $\to$ mônica, retração $\to$ épica, seção e retração $\to$ isomorfismo, etc).

Exemplo 2.3.2. Em Conj, $R{-}\mathsf{Mod}$, Grp, $R{-}\mathsf{Alg}$, os monomorfismos são precisamente os mapas injetivos. Em Conj e $R{-}\mathsf{Mod}$, os epimorfismos são precisamente os mapas sobrejetivos; em Grp também, mas é prova é sutil; em $R{-}\mathsf{Alg}$ há epimorfismos não sobrejetivos, como $R[X] \to R[X, X^{-1}]$.

2.4 Transformações naturais

Definição 2.4.1. Dados functores $F, G : \mathcal{A} \to \mathcal{C}$, uma "transformação natural" $\eta : F \implies G$ consiste de setas $\eta_A : F(A) \to G(A)$ (para cada $A \in \mathcal{A}$), satisfazendo

$$\forall_{A,B\in\mathcal{A}} \forall_{f\in\mathcal{C}(A,B)} G(f) \circ \eta_A = \eta_B \circ F(f),$$

que num diagrama comutativo se escreve:

$$\begin{array}{ccc} F(A) & \xrightarrow{\eta_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow[\eta_B]{} & G(B) \end{array}$$

Exemplo 2.4.2. Se $F : R{-}\mathsf{Alg} \to \mathsf{Conj}$ é o functor que esquece a estrutura de álgebra, há transformação natural $\eta : F \implies F$ dada, digamos, por $\eta_A(x) \coloneqq x^{123} + 321$. E sendo $I : K{-}\mathsf{Vect} \to K{-}\mathsf{Vect}$ o functor identidade e $E : K{-}\mathsf{Vect} \to K{-}\mathsf{Vect}$ o duplo dual, $E(V) \coloneqq V^{**}$, há transformação natural $\theta : I \to E$, $\theta_V(x) \coloneqq (f \mapsto f(x))$; logo, se $\dim V < \infty$, $V \cong V^{**}$ "naturalmente", de fato como na intuição.

Definição 2.4.3. Se $\mathcal{I}$ é categoria "pequena", e dada categoria $\mathcal{C}$, pode-se definir a categoria $\mathcal{C}^{\mathcal{I}}$, cujos objetos são os functores (diagramas) $\mathcal{I} \to \mathcal{C}$, e tais que cada $\mathcal{C}^{\mathcal{I}}(F, G)$ consiste das transformações naturais $F \implies G$ (com identidades e composições provenientes das de $\mathcal{C}$).

Há muitas transformações naturais no texto, porém muitas vezes deixarei implícito quais as categorias e quais os functores envolvidos.

2.4.1 Tipos de functores, equivalência

Definição 2.4.4. Um functor $F : \mathcal{A} \to \mathcal{B}$ é dito ser:

- "fiel" quando cada ação $F : \mathcal{A}(X, Y) \to \mathcal{B}(FX, FY)$ é injetiva;
- "pleno" quando cada ação $F : \mathcal{A}(X, Y) \to \mathcal{B}(FX, FY)$ é sobrejetiva.

Fato 2.4.5 (Functor pleno, fiel e essencialmente sobrejetivo é equivalência)**.** *Se $F : \mathcal{A} \to \mathcal{B}$ é functor pleno e fiel, se $|G| : \mathcal{B} \to \mathcal{A}$ é função nos objetos, com família de isomorfismos $\phi_B : B \cong F\left(|G|\left(B\right)\right)$, então sendo*

$$G\left(B \xrightarrow{g} B'\right) \coloneqq F^{-1}_{|G|(B),|G|(B')}\Big(F\left(|G|\left(B\right)\right) \xrightarrow{\phi_B^{-1}} B \xrightarrow{g} B' \xrightarrow{\phi_{B'}} F\left(|G|\left(B'\right)\right)\Big),$$

temos que $G : \mathcal{B} \to \mathcal{A}$ é functor com $F \circ G \cong 1_{\mathcal{B}}$ e $G \circ F \cong 1_{\mathcal{A}}$, isto é, F é uma "equivalência de categorias".

Uma equivalência de categorias preserva todas as propriedades formuladas em termos de igualdades e composições de setas, mas não precisa preservar a "igualdade de objetos".

2.5 Lema de Yoneda

Fato 2.5.1. *Dado functor $F : \mathcal{A} \to \mathsf{Conj}$, dado objeto $A \in \mathcal{A}$, dada transformação natural $\eta : \hom(A, \_) \implies F$, existe único $a \in F(A)$ tal que $\forall_{(B \in \mathcal{A})} \eta_B(A \xrightarrow{f} B) = F(f)(a)$.*

Brevemente $(\hom(A, \_) \implies F) \cong F(A)$.

2.6 Limites e colimites

Definição 2.6.1. Dado um diagrama (functor) $F : \mathcal{I} \to C$, um "limite" para F consiste de $L \in \mathcal{C}$ e $\kappa : \Delta(L) \implies F$ (chamada "cone universal"), onde $\Delta(L) : \mathcal{I} \to \mathcal{C}$ é o functor-constante, tal que:

$$\forall\left(\lambda{:}\Delta(A) \overset{A\in\mathcal{C}}{\Longrightarrow} F\right)\ \exists!(f : A \to L)\ \lambda = \kappa \circ \Delta(f).$$

(Escreve-se $f = (\lambda)_\kappa$.) Diz-se que um limite é finito, enumerável, etc., quando $\mathcal{I}$ é categoria com número finito, enumerável, etc., de setas.

Exemplo 2.6.2. Quando $\mathcal{I} = \{0\ 1\}$ (dois objetos, sem setas não identidades), um limite para $F : \mathcal{I} \to \mathcal{C}$ é o mesmo que um "produto binário" de $F(0)$ e $F(1)$: objeto L e setas $\pi_i : L \to F(i)$ tais que, para quaisquer $a : X \to A$ e $b : X \to B$, existe única $(a, b) : X \to L$ tal que $\pi_0 \circ (a, b) = a$ e $\pi_1 \circ (a, b) = b$.

Definição 2.6.3. O colimite é definido dualmente: um "colimite" de $F : \mathcal{I} \to \mathcal{C}$ consiste de $L \in \mathcal{C}$ e $\kappa : F \implies \Delta(L)$ ("cocone universal") tal que $\forall(A \in \mathcal{C})\ \forall(\lambda : F \implies \Delta(A))\ \exists!(f : C \to A)\ \lambda = \Delta(f) \circ \kappa$. (Escreve-se $f = \langle\lambda\rangle_\kappa$.)

Vários limites e colimites têm nomes especiais:

$\mathcal{I}$	nome do limite	nome do colimite
vazia	objeto final (1)	objeto inicial (0)
$\{0\ 1\ \cdots (N-1)\}$	produto N-ário ($\times$)	coproduto N-ário ($\sqcup$)
$\{0 \rightrightarrows 1\}$	equalizador	coequalizador
$\{0 \to V \leftarrow 1\}$	produto fibrado	—
$\{0 \leftarrow V \to 1\}$	—	soma amalgamada /coproduto fibrado
pré-ordem	limite inverso/projetivo	limite(!) direto/indutivo

Observação 2.6.4. Há uma construção explícita para limites e colimites em Conj (e categorias similares).

O limite de $F : \mathcal{I} \to \mathsf{Conj}$ é dado por um subconjunto dum produto:

$$\lim F \coloneqq \left\{(a_i)_{i\in\mathcal{I}} \mid \forall_{f:i\to j} F(f)(a_i) = a_j\right\},$$

onde o cone $\kappa : \Delta(\lim F) \implies F$ é dado pelas projeções.

O colimite de $F : \mathcal{I} \to \mathsf{Conj}$ é dado por um quociente duma soma:

$$\operatorname{co\lim} F \coloneqq \left(\coprod_{i\in\mathcal{I}} F(i)\right)/\!\sim,$$

onde $\sim$ é a relação de equivalência gerada por cada $\iota_i(a_i) \sim \iota_j(F(f)(a_j))$, para cada $f : i \to j$. (Aqui $\coprod_{i\in\mathcal{I}} F(i)$ é a união disjunta $\bigcup_{i\in\mathcal{I}}\{i\} \times F(i)$, e $\iota_i(a) = (i, a)$.) (Se trocarmos Conj por

Grp, por exemplo, trocamos $\coprod$ pelo produto livre de grupos, e $\sim$ pelo menor subgrupo normal incluindo cada $\iota_i(a_i)^{-1}\iota_j\left(F(f)(a_j)\right)$.)

Mais geralmente, se existem todos os (co) produtos finitos e (co) equalizadores, existem todos os (co) limites finitos.

Como casos importantes, em $R-\mathsf{Alg}$, o objeto final é 0, o inicial é R; o produto é o produto usual, o coproduto é o produto tensorial $\otimes_R$; o equalizador de $f, g : A \to B$ é a subálgebra $\{x \mid f(x) = g(x)\}$, o coequalizador é o quociente de B pelo ideal gerado por $\{x \mid f(x) - g(x)\}$; o produto fibrado de $A \xrightarrow{f} V \xleftarrow{g} B$ é $\{(x, y) \in A \times B \mid f(x) = g(y)\}$; a soma amalgamada de $A \xleftarrow{f} V \xrightarrow{g} B$ é $A \otimes_V B$ (somas de tensores satisfazendo $a \cdot f(v) \otimes b = a \otimes g(v) \cdot b$).

Uma notação muito usada será: para $f : A \to C$ e $g : B \to C$, $\langle f, g\rangle : A \otimes B \to C$, $\langle f, g\rangle(a \otimes b) \coloneqq fa \cdot gb$, um caso particular da notação acima de colimite.

Limites (e colimites) são "functoriais": se $\eta : F \implies F'$ e há limites $\kappa : \Delta(L) \implies F$ e $\kappa' : \Delta(L') \implies F'$, então há única $\lim \eta : L \to L'$ tal que $\eta \circ \kappa = \kappa' \circ \Delta(\lim \eta)$.

2.7 Adjunções

Definição 2.7.1. Uma "adjunção" $F \dashv G$ consiste de functores $F : \mathcal{A} \to \mathcal{B}$ e $G : \mathcal{B} \to \mathcal{A}$ e uma transformação natural:

$$\phi : \mathcal{B}\left(F(\_), \_\right) \cong \mathcal{A}\left(\_, G(\_)\right) : \mathcal{A}^\circ \times \mathcal{B} \to \mathsf{Conj}.$$

Sua "unidade" η e "counidade" ϵ são dadas por: $\eta : 1_{\mathcal{A}} \implies G \circ F$, $\eta_A \coloneqq \phi_{A,F(A)}\left(1_A\right)$; $\epsilon : F \circ G \implies 1_{\mathcal{B}}$, $\epsilon_B \coloneqq \phi^{-1}_{G(B),B}\left(1_B\right)$.

Fato 2.7.2. *Na adjunção acima, temos:*

(a) (naturalidade) $\phi(FA \xrightarrow{f} B) = A \xrightarrow{\eta_A} GFA \xrightarrow{Gf} GB$, $\phi^{-1}(A \xrightarrow{g} GB) = FA \xrightarrow{Fg} FGB \xrightarrow{\epsilon_B} B$;

(b) (identidades triangulares) $\epsilon F \circ F\eta = 1_F$ *e* $G\epsilon \circ \eta G = 1_G$.

Fato 2.7.3. *Na adjunção* $F \dashv G$ *acima:*

(a) ("adjunto direito preserva limites") se temos $\kappa : \Delta(L) \implies H : \mathcal{I} \to \mathcal{B}$ *cone universal, então* $G\kappa : \Delta(GL) \implies GH : \mathcal{I} \to \mathcal{A}$ *é cone universal também;*

(b) ("adjunto esquerdo preserva colimites") se temos $\kappa : H \implies \Delta(C) : \mathcal{I} \to \mathcal{A}$ *cocone universal, então* $F\kappa : FH \implies \Delta(FC) : \mathcal{I} \to \mathcal{B}$ *é cocone universal também.*

Exemplo 2.7.4. Temos a adjunção "tensor-hom":

$$K-\mathsf{Vect}\left(\_ \otimes B, \_\right) \cong K-\mathsf{Vect}\left(\_, \hom_K(B, \_)\right).$$

Logo temos que $\_ \otimes B$ preserva todos os colimites e $\hom_K(B, \_)$ preserva todos os limites. Notar:

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \text{ exata à esquerda } \iff f \text{ é equalizador de } g, 0$$

$$A \xrightarrow{f} B \xrightarrow{g} C \to 0 \text{ exata à direita } \iff f \text{ é coequalizador de } g, 0$$

Logo tensor é functor exato direito e hom é exato esquerdo.

Exemplo 2.7.5. Quando $\mathcal{A}$ e $\mathcal{B}$ são pré-ordens, uma adjunção é o mesmo que: $FA \leq B \iff A \leq GB$ (que implica F e G serem functores, isto é, "crescentes"). Logo, se as pré-ordens são antissimétricas, temos as identidades triangulares $FA = FGFB$, $GB = GFGB$. Um limite numa ordem é um ínfimo e que um colimite é um supremo, logo, se $\sup_i A_i$ e $\inf_j B_j$ existirem, $\sup_i F(A_i) = F(\sup_i A_i)$, $\inf_j G(B_j) = G(\inf_j B_j)$.

2.8 Objetos-grupos

Definição 2.8.1. Seja $\mathcal{C}$ uma categoria com todos os produtos finitos de seus objetos (incluindo o produto nulário 1, que é o objeto final). Um "objeto-grupo" consiste dum objeto G e de setas $e : 1 \to G$, $i : G \to G$ e $m : G \times G \to G$ tais que os diagramas abaixo comutam:

$$\text{(elemento neutro) } G \xrightarrow{(e,())} G \times G \xleftarrow{((),e)} G, \quad G \xrightarrow{m} G \text{ via } 1 \text{ e } 1$$

$$\text{(inversos) } G \xrightarrow{(1,i)} G \times G \xleftarrow{(i,1)} G, \quad G \xrightarrow{()} 1 \xrightarrow{e} G \text{ e } G \xrightarrow{m} G \xrightarrow{()} 1 \xrightarrow{e} G$$

$$\text{(associatividade) } (G \times G) \times G \xrightarrow{\alpha} G \times (G \times G), \quad m \times 1 : (G \times G) \times G \to G \times G, \quad 1 \times m : G \times (G \times G) \to G \times G, \quad m : G \times G \to G, \quad m : G \times G \to G, \quad m : G \to G \text{ e } m : G \to G$$

onde α é o "associador" $(p \circ p, (q \circ p, q))$, onde $p, q : (\cdots) \times (\cdots) \to (\cdots)$ são as duas projeções.

Todas as provas na teoria dos grupos dadas por uma mera sequência de igualdades se aplicam também a objetos-grupos.

Por exemplo, podemos provar $(ab)^{-1} = b^{-1}a^{-1}$ assim:

$$\begin{aligned} b^{-1}a^{-1} &= e(b^{-1}a^{-1}) = ((ab)^{-1}(ab))(b^{-1}a^{-1}) = (ab)^{-1}\left((ab)(b^{-1}a^{-1})\right) \\ &= (ab)^{-1}\left(a(b(b^{-1}a^{-1}))\right) = (ab)^{-1}\left(a((bb^{-1})a^{-1})\right) = (ab)^{-1}\left(a(ea^{-1})\right) \\ &= (ab)^{-1}\left(aa^{-1}\right) = (ab)^{-1}e = (ab)^{-1}. \end{aligned}$$

A afirmação similar para objetos-grupos $i \circ m = m \circ (i \circ q, i \circ p)$ pode ser provada trocando as variáveis a, b pelas respectivas projeções p, q, trocando as operações por e, i, m, e usando $p(f, g) = f$, $q(f, g) = g$ e $(ph, qh) = h$.

Definição 2.8.2. Dada categoria $\mathcal{A}$, a "categoria dos objetos-grupos" $\mathsf{Grp}(\mathcal{A})$ de $\mathcal{A}$ consiste dos objetos-grupo (G, e, i, m), com setas:

$$\mathsf{Grp}(\mathcal{A})\left((G, e, i, m), (G', e', i', m')\right) \coloneqq \{f \in \mathcal{A}(G, G') \mid f \circ m = m' \circ (f \times f)\}.$$

(A condição $f \circ m = m' \circ (f \times f)$ implica $f \circ e = e'$ e $f \circ i = i' \circ f$.)

2.9 Categorias abelianas

Denota-se por $R-\mathsf{Mod}$ a categoria dos módulos sobre um anel (não necessariamente comutativo nem unitário) R.

Definição 2.9.1. Uma "categoria pré-aditiva" consiste duma categoria $\mathcal{C}$ e família de operações $(+) : \mathcal{C}(A, B) \times \mathcal{C}(A, B) \to \mathcal{C}(A, B)$ tornando os conjuntos hom grupos abelianos para os quais as composições $\circ$ são biaditivas.

Há então setas nulas $0 : A \to B$. Chama-se "núcleo" de f um equalizador de f e 0, e chama-se "conúcleo" de f um coequalizador de f e 0.

Se uma categoria pré-aditiva tem um objeto inicial 0, isto é há única seta $0 \to A$ para cada objeto A, temos em particular $1_0 = 0 : 0 \to 0$; assim 0 é objeto final também, pois $\forall_{f:A\to 0} f = 1_0 \circ f = 0 \circ f = 0$.

Definição 2.9.2. Dada categoria pré-aditiva $\mathcal{A}$, um "diagrama de soma direta" para $A, B \in \mathcal{A}$ consiste de setas $A \underset{i_1}{\overset{p_1}{\leftrightarrows}} C \underset{i_2}{\overset{p_2}{\rightleftarrows}} B$ satisfazendo $p_1 \circ i_1 = 1_A$, $p_2 \circ i_2 = 1_B$ e $i_1 \circ p_1 + i_2 \circ p_2 = 1_C$.

Em particular, $p_1 \circ i_2 = p_1 \circ (i_1 \circ p_1 + i_2 \circ p_2) \circ i_2 = 1 \circ p_1 \circ i_2 + p_1 \circ i_2 \circ 1$, logo $p_1 \circ i_2 = 0$, e similarmente $p_2 \circ i_1 = 0$. Pode-se mostrar que C é simultaneamente produto e coproduto de A, B; escreve-se $C \coloneqq A \oplus B$.

Definição 2.9.3. Uma "categoria abeliana" $\mathcal{C}$ consiste duma categoria pré-aditiva $\mathcal{C}$:

- com um objeto inicial (que também será final) 0;

- com somas diretas $A \oplus B$ para quaisquer dois objetos A, B;
- com núcleo $\operatorname{nuc} f : Nf \to A$ para cada seta $f : A \to B$;
- com conúcleo $\operatorname{conuc} g : B \to Cg$ para cada seta $g : A \to B$;
- e tal que todo monomorfismo é núcleo e todo epimorfismo é conúcleo.

$R-\mathsf{Mod}$ é o primeiro exemplo de categoria abeliana. Mostremos como toda categoria abeliana pode ser manipulada como se fosse uma categoria de módulos.

Lema 2.9.4. *Temos adjunção*

$$\operatorname{nuc} f \succeq^{\to A} g \iff f \preceq^{A\to} \operatorname{conuc} g$$

entre functores $\operatorname{nuc} : (A \to) \leftrightarrow (\to A) : \operatorname{conuc}$*, onde* $(A \to)$ *denota a família de setas de domínio* A *e* $(\to A)$ *denota a família de setas de contradomínio* A*, e onde*

$$f \preceq^{A\to} f' \iff \exists_k f = k \circ f', \quad g \preceq^{\to A} g' \iff \exists_k g = g' \circ k.$$

Em particular, numa categoria abeliana, se f *é monomorfismo e* g *é epimorfismo, existem* ϕ *e* ψ *isomorfismos com*

$$f = \operatorname{nuc}\operatorname{conuc} f \circ \phi, \quad g = \psi \circ \operatorname{conuc}\operatorname{nuc} g.$$

(Isto é, cada monomorfismo é núcleo de seu conúcleo, e cada epimorfismo é conúcleo de seu núcleo).

Demonstração. É fácil ver que $\preceq^{A\to}$ e $\preceq^{\to A}$ são pré-ordens. Pela definição de núcleo e conúcleo,

$$\begin{aligned}\operatorname{nuc} f \succeq^{\to A} g &\iff \exists_k g = \operatorname{nuc} f \circ k \iff f \circ g = 0 \\ &\iff \exists_k f = k \circ \operatorname{conuc} g \iff f \preceq^{A\to} \operatorname{conuc} g.\end{aligned}$$

Agora, se $f : (\cdots) \to A$ é monomorfismo, a definição de categoria abeliana diz que f é um núcleo de alguma h, e como limites são únicos, existe isomorfismo α com $f = \operatorname{nuc} h \circ \alpha$, e $f \circ \alpha^{-1} = \operatorname{nuc} h$; assim $f \preceq^{\to A} \operatorname{nuc} h \preceq^{\to A} f$ (brevemente $f \equiv^{\to A} \operatorname{nuc} h$). Pela identidade triangular de adjunções,

$$\operatorname{nuc} h \equiv^{\to A} \operatorname{nuc}\operatorname{conuc}\operatorname{nuc} h \implies f \equiv^{\to A} \operatorname{nuc}\operatorname{conuc} f,$$

logo existem β e γ com $f \circ \beta = \operatorname{nuc}\operatorname{conuc} f$ e $f = \operatorname{nuc}\operatorname{conuc} f \circ \alpha$. Notar que

$$f \circ \beta \circ \alpha = f, \ \operatorname{nuc}\operatorname{conuc} f \circ \alpha \circ \beta = \operatorname{nuc}\operatorname{conuc} f,$$

e como f e o núcleo são monomorfismos, vale $\beta \circ \alpha = 1$ e $\alpha \circ \beta = 1$; logo $\phi := \alpha$ é isomorfismo, como desejado. (A segunda propriedade, de g epimorfismo, é simétrica). □

Chama-se uma seta $x : X \to A$ de "elemento generalizado" de A. Dizemos que dois elementos generalizados $x : X \to A$ e $y : Y \to A$ são "equivalentes" (escrito $x \equiv y$) quando há epimorfismos $X \xleftarrow{p} W \xrightarrow{q} Y$ com $xp = yq$.

Lema 2.9.5. *$\equiv$ é relação de equivalência numa categoria abeliana.*

Prova da transitividade. Sejam p, q, q', r' epimorfismos com $xp = yq$ e $yq' = zr'$ como em:

$$\begin{array}{ccccc} W'' & \xrightarrow{Q'} & W & \xrightarrow{p} & X \\ {\scriptstyle Q}\downarrow & & \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle x} \\ W' & \xrightarrow{q'} & Y & \xrightarrow{y} & A \\ {\scriptstyle r'}\downarrow & & \downarrow{\scriptstyle y} & & \\ Z & \xrightarrow[z]{} & A & & \end{array}$$

Como $\mathcal{A}$ tem todos os limites finitos (tem produtos e equalizadores), pode-se tomar W'' produto fibrado como no diagrama.

Pode-se mostrar que q (resp., q') ser epimorfismo implica Q (resp., Q') epimorfismo:

- temos núcleo
$$W'' \xrightarrow{(Q',Q)} W \oplus W' \xrightarrow{qp_1 - q'p_2} Y$$
pela construção dos limites em termos de produtos e equalizadores;
- $qp_1 - q'p_2$ é epimorfismo, porque
$$0 = f\,(qp_1 - q'p_2) \implies 0 = f\,(qp_1 - q'p_2)\,i_1 = fq \implies 0 = f$$
pois q é epimorfismo;
- assim $qp_1 - q'p_2$ é conúcleo de seu núcleo (Q', Q);
- enfim, se $fQ = 0$, vale $fp_2(Q', Q) = 0$, logo há k com $fp_2 = k(qp_1 - q'p_2)$, logo $0 = fp_2i_1 = kq$, e q é epimorfismo, logo $k = 0$ e $f = 0$.

Então $x \equiv z$ porque $x(pQ') = z(r'Q)$. □

Fato 2.9.6. *Numa categoria abeliana $\mathcal{A}$:*

1. *$f : A \to B$ é monomorfismo sse $\forall_X \forall_{x:X\to A} fx \equiv 0 \implies x \equiv 0$;*
2. *$g : A \to B$ é epimorfismo sse $\forall_Y \forall_{y:Y\to B} \exists_{x:X\to A} gx \equiv y$.*

3. *se* $f : A \to B$ *é monomorfismo,* f *é núcleo de* $g : B \to C$ *sse* $\forall_{x:X\to B} gx \equiv 0 \iff \exists_{x':X\to A} x \equiv fx'$.

4. *dados* $x : X \to A$ *e* $y : Y \to A$*, há* $x', y' : Z \to A$ *(de mesmo domínio) com* $x \equiv x'$ *e* $y \equiv y'$.

Demonstração. (1→) Se $fx \equiv 0$, há épica q com $fxq = 0$, logo $xq = 0$ pois f é mônica, logo $x \equiv 0$.

(1←) Se $fg = 0$, em particular $fg \equiv 0$, logo $g \equiv 0$, há épica q com $gq = 0 = 0q$, logo $g = 0$.

(2→) Dada $y : Y \to B$, considere produto fibrado como em

$$\begin{array}{ccc} W & \overset{g'}{\twoheadrightarrow} & Y \\ {\scriptstyle x}\downarrow & & \downarrow{\scriptstyle y} \\ A & \underset{g}{\twoheadrightarrow} & B \end{array}$$

então g ser epimorfismo implica que g' é epimorfismo, logo $gx = yg' \equiv y$.

(2←) Se $fg = 0$, existe x com $gx \equiv 1$, logo há epimorfismos p, q com $gxp = q$, logo $fq = 0$, logo $f = 0$.

(3→) Se $gx \equiv 0$, temos $gx = 0$ como no item (1), logo x se fatora unicamente como fx'; e se $x \equiv fx'$, temos $gx \equiv gfx' = 0$.

(3←) Primeiro, $f \equiv f1$, logo $gf \equiv 0$, logo $gf = 0$. Assim, sendo $x : X \to B$ núcleo de g, temos fatoração $f = xy$, em particular y é mônica (pois é fator direito em fatoração de mônica f); a hipótese com $gx = 0$ dá $x \equiv fx' = xyx'$; como x é mônico, $1 \equiv yx'$, logo y é épica (pois é fator esquerdo de fatoração de épica); assim, y é isomorfismo (pois é núcleo épico), e f também é núcleo de g.

(4) $xp_X : X \times Y \to A$, $yp_Y : X \times Y \to A$ e p_X, p_Y são épicas. □

Assim, é justificado definir que uma sequência $A \xrightarrow{f} B \xrightarrow{g} C$ é "exata" em B quando $gf = 0$ e

$$\forall_X \forall_{x:X\to B} gx \equiv 0 \implies \exists_Y \exists_{y:Y\to A} fy \equiv x.$$

É possível então redemonstrar, em qualquer categoria abeliana, o lema da cobra, o lema dos cinco, etc. (Esses são lemas básicos da álgebra homológica, afirmando que em certas condições que certos mapas são mônicos ou épicos, e tendo fáceis provas por meio das propriedades básicas acima).

2.9.1 Ações em sequências exatas

Lema 2.9.7. *Dado diagrama de soma amalgamada*

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & A' \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi'} \\ B & \xrightarrow[\beta]{} & B' \end{array}$$

(a) se α é epimorfismo, β também é; (b) se a categoria é abeliana e α é monomorfismo, β também é.

Demonstração. (a) Sejam $\pi, \sigma : B' \to X$ com $\pi\beta = \sigma\beta$; logo, $\pi\phi'\alpha = \pi\beta\phi = \sigma\beta\phi = \sigma\phi'\alpha$; como α é epimorfismo, $\pi\phi' = \sigma\phi'$; como B' é soma amalgamada, $\pi = \sigma$.

(b) Na prova do lema 2.9.5, foi provada a afirmação dual (sobre produtos fibrados e epimorfismos); pode ser aplicada porque dual de categoria abeliana é abeliana. □

Teorema 2.9.8. *Numa categoria abeliana, dado diagrama comutativo:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & A' & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & B & \longrightarrow & B' & \longrightarrow & A'' & \longrightarrow & 0 \end{array}$$

onde a primeira linha é exata e a segunda linha é um complexo de cadeia, equivalem-se: (a) o quadrado $AA'BB'$ é uma soma amalgamada; (b) a segunda linha é exata também.

Demonstração. (a) Pelo lema anterior, como $A \to A'$ é mônica, $B \to B'$ é mônica. E como $\begin{smallmatrix} A' \\ \downarrow \\ B' \to A'' \end{smallmatrix} = (A' \to A'')$ é épica, seu fator esquerdo $B' \to A''$ é épica. Resta provar exatidão em B'.

Seja $B' \to X$ tal que $(B \to B' \to X) = 0$. Vale $\begin{smallmatrix} A \to A' \\ \downarrow \\ B' \to X \end{smallmatrix} = \begin{smallmatrix} A \\ \downarrow \\ B \to B' \to X \end{smallmatrix} = 0$, e pela exatidão em A', existe $A'' \to X$ tal que $\begin{smallmatrix} A' \\ \downarrow \\ B' \to X \end{smallmatrix} = \begin{smallmatrix} A' \to A'' \\ \searrow \\ X \end{smallmatrix}$, também igual a $\begin{smallmatrix} A' \\ \downarrow \\ B' \to A'' \to X \end{smallmatrix}$. Lembrando que $(B \to B' \to X) = 0 = (B \to B' \to A'' \to X)$, vale que $(B' \to X)$ e $(B' \to A'' \to X)$ têm iguais composições com os mapas da soma amalgamada, logo $(B' \to X) = (B' \to A'' \to X)$.

(b→a) No diagrama abaixo, S é a soma amalgamada como em (a) (logo a

linha do meio é exata) e a seta $S \to B'$ é definida de modo que tudo comute:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & A' & \longrightarrow & A'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & B & \longrightarrow & S & \longrightarrow & A'' & \longrightarrow & 0 \\
 & & \| & & \vdots & & \| & & \\
0 & \longrightarrow & B & \longrightarrow & B' & \longrightarrow & A'' & \longrightarrow & 0
\end{array}$$

Por um lema básico de homologia (fácil de provar com elementos generalizados), $S \to B'$ é isomorfismo, logo B' é soma amalgamada. □

Definição 2.9.9. Numa categoria abeliana, define-se $\mathrm{Ext}^1(B, A)$ como a "família" das sequências exatas $0 \to A \to * \to B \to 0$ (atenção à ordem!) módulo a relação de equivalência: $(0 \to A \to X \to B \to 0) \equiv (0 \to A \to X' \to B \to 0)$ sse existe isomorfismo $X \cong X'$ de modo que os triângulos AXX' e $XX'B$ comutem.

Assim, pelo teorema anterior, $\mathrm{Ext}^1(\_, \_)$ é functor contravariante na segunda componente (usando somas amalgamadas), e similarmente na primeira (usando produtos fibrados). (Na prova da regra de composição de functores, usa-se que dois diagramas de somas amalgamadas adjacentes formam outro diagrama de mesmo tipo).

Definição 2.9.10. Dadas sequências exatas $E \coloneqq (0 \to A \to X \to B \to 0)$ e $E' \coloneqq (0 \to A' \to X' \to B' \to 0)$, definimos $E \oplus E' \in \mathrm{Ext}^1(B \oplus B', A \oplus A')$ como a sequência exata $(0 \to A \oplus A' \to X \oplus X' \to B \oplus B' \to 0)$.

No caso $A = A'$ e $B = B'$, definimos $E + E' \in \mathrm{Ext}^1(B, A)$ como $E + E' \coloneqq \mathrm{Ext}^1\left(B \overset{\delta \coloneqq \langle 1,1 \rangle}{\to} B \oplus B, A \oplus A \overset{(+)}{\to} A\right)(E \oplus E')$. (Fácil de ver que preserva $\equiv$.)

Fato 2.9.11. *Numa categoria abeliana, cada* $\mathrm{Ext}^1(B, A)$ *tem estrutura de grupo abeliano, cujo elemento neutro é* $0_{\mathrm{Ext}(B,A)} \coloneqq (0 \to A \to A \oplus B \to B \to 0)$ *(sequência cindível), de modo que* $\mathrm{Ext}^1(\_, \_)$ *seja functor biaditivo.*

Demonstração. Usaremos implicitamente propriedades básicas de somas amalgamadas e produtos fibrados. Abreviando a ação de Ext^1 por $*$, temos $(E + E') + E'' \coloneqq (+) * \Big(\big((+) * (E \oplus E') * \delta\big) \oplus E''\Big) * \delta \equiv (+) * ((+) \oplus 1) * \big((E \oplus E') \oplus E''\big) * (\delta \oplus 1) * \delta \equiv (+)_3 * (E \oplus E' \oplus E'') * \delta_3$, dando associatividade. E há diagrama comutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & X & \longrightarrow & B & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle 0} & & \downarrow & & \| & & \\
0 & \longrightarrow & A & \longrightarrow & A \oplus B & \longrightarrow & B & \longrightarrow & 0
\end{array}$$

logo pelo teorema anterior $E * 0 = 0_{\mathrm{Ext}(B,A)}$; e $E * f + E * g \equiv E * (f + g)$ dá que $E * 0$ é elemento neutro, e $E * (-1)$ é oposto. □

Lema 2.9.12. *Se* $0 \to A \to B \to C \to 0$ *é sequência exata numa categoria abeliana e* X *é outro objeto, a sequência induzida* $\mathrm{Ext}^1(C,X) \to \mathrm{Ext}^1(B,X) \to \mathrm{Ext}^1(A,X)$ *é exata.*

Demonstração. A composta é nula pois $\mathrm{Ext}^1(\_,X)$ é functor. Seja $(0 \to X \to Y \to B \to 0)$ cuja imagem em $\mathrm{Ext}^1(A,X)$ se anula (dá a sequência cindível). Assim, há diagrama comutativo, com produto fibrado no quadrado direito superior, e queremos encontrar Z e os três mapas tracejados abaixo:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X & \longrightarrow & X \oplus A & \longrightarrow & A & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & B & \longrightarrow & 0 \\
 & & \| & & \vdots & & \downarrow & & \\
0 & \longrightarrow & X & \dashrightarrow & (Z) & \dashrightarrow & C & \longrightarrow & 0
\end{array}$$

Temos o mapa $A \to X \oplus A \to Y$; pomos em $Y \to Z$ o seu conúcleo. O mapa $X \to Z$ é definido como a composta $X \to Y \to Z$. O mapa $Z \to C$ é definido como a fatoração de $(Y \to B \to C)$ pelo conúcleo $Y \to Z$ (porque $(A \to Y \to C) = (A \to B \to C) = 0$).

A composta de baixo anula-se pois $(X \to Z \to C) = (X \to Y \to B \to C) = 0$.

Se há $W \to X$ com $(W \to X \to Z) = 0$, então $W \to X \to Y$ se fatora pelo núcleo de $Y \to Z$, que é $A \to Y$ (porque este é mônico, porque $X \oplus A \to Y$ o é, pelo lema 2.9.7 (dual) aplicado a $A \to B$). Assim, $(W \to X \to Y) = (W \dashrightarrow A \to Y)$, o que dá mapa $(W \overset{\dashrightarrow}{\to} X \oplus A \to Y) = 0$, e como $X \oplus A \to Y$ é mônico, $(W \overset{\dashrightarrow}{\to} X \oplus A) = 0$, e $(W \to X) = 0$. Então $X \to Z$ é mônico.

$Z \to C$ é épico porque $(Y \to Z \to C) = (Y \to B \to C)$ o é (composição de dois épicos).

Seja t tal que $f_{Z\to C}t \equiv 0$; como $Y \to Z$ é um conúcleo, há y tal que $t \equiv f_{Y\to Z}y$; logo, $0 \equiv f_{Y\to C}y = f_{B\to C}(f_{Y\to B}y)$; como $(0 \to A \to B \to C \to 0)$ é exata, há a com $f_{Y\to B}y \equiv f_{A\to B}a$; troque y, a por equivalentes de um mesmo domínio para ambos; logo, $f_{Y\to B}(f_{A\to Y}a) \equiv f_{A\to B}a \equiv f_{Y\to B}y$, e há x com $y - f_{A\to Y}a \equiv f_{X\to Y}x$; assim $f_{X\to Z}x \equiv f_{Y\to Z}(f_{X\to Y}x) \equiv f_{Y\to Z}(y - f_{A\to Y}a) \equiv f_{Y\to Z}y - 0 \equiv t$.

Portanto, a linha de baixo é exata também, o que mostra que $(0 \to X \to Y \to Z \to 0)$ está na imagem de $\mathrm{Ext}^1(C,X)$. □

Lema 2.9.13. *Dada sequência exata* $E \coloneqq (0 \to A \overset{f}{\to} B \overset{g}{\to} C \to 0)$ *numa categoria abeliana, vale que* $\mathrm{Ext}^1(1,f)(E) = 0 \in \mathrm{Ext}^1(C,B)$.

Demonstração. A sequência exata $\mathrm{Ext}^1(1,f)(E)$ é $0 \to B \to X \to C \to 0$ onde X é soma amalgamada de $f : A \to B$ com o mesmo f; pode-se ver que $X \cong B \oplus C$, com

os dois mapas $B \to B \oplus C$ sendo ι_0 e $\iota_0 + \iota_1 \circ g$; então $0 \to B \to X \to C \to 0$ é a sequência cindível. □

Lema 2.9.14. *Se* $E \coloneqq (0 \to A \to B \to C \to 0)$ *é sequência exata numa categoria abeliana e* X *é outro objeto, a sequência induzida* $\hom(A, X) \overset{\mathrm{Ext}^1(1,\_)E}{\to} \mathrm{Ext}^1(C, X) \to \mathrm{Ext}^1(B, X)$ *é exata.*

Demonstração. Denotando $A \overset{f}{\to} B \overset{g}{\to} C$, a composta é $h \mapsto \mathrm{Ext}^1(g, 1)(\mathrm{Ext}^1(1, h)E) = \mathrm{Ext}^1(1, h)(\mathrm{Ext}^1(g, 1)E) = 0$, pelo lema anterior (na categoria dual). Seja agora $E' \coloneqq (0 \to X \to Y \to C \to 0) \in \mathrm{Ext}^1(C, X)$ com $\mathrm{Ext}^1(g, 1)E' = 0$; logo o primeiro diagrama comuta:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \longrightarrow & X \oplus B & \longrightarrow & B & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & C & \longrightarrow & 0 \end{array} \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle h} & & \downarrow & & \| & & \\ 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

logo, temos $A \to B \to X \oplus B \to Y$, que composto com $Y \to C$ é $A \to B \to C$, zero; logo, $A \to B \to X \oplus B \to Y$ fatora-se unicamente como $A \overset{h}{\to} X \to Y$; o segundo diagrama comuta, logo $\mathrm{Ext}^1(1, h)E = E'$. □

Lema 2.9.15. *Se* $E \coloneqq (0 \to A \to B \to C \to 0)$ *é sequência exata numa categoria abeliana e* X *é outro objeto, a sequência induzida* $\hom(B, X) \to \hom(A, X) \overset{\mathrm{Ext}^1(1,\_)E}{\to} \mathrm{Ext}^1(C, X)$ *é exata.*

Demonstração. Sendo $A \overset{f}{\to} B \overset{g}{\to} C$, composta é $k \mapsto \mathrm{Ext}^1(1, k)(\mathrm{Ext}^1(1, f)E) = 0$. Seja agora $h \in \hom(A, X)$ com $\mathrm{Ext}^1(1, h)E = 0$. Logo, temos $B \to X \oplus C \to X$, onde $A \to B \to X \oplus C \to X$ é h; então h está na imagem de $\hom(B, X) \to \hom(A, X)$. □

Capítulo 3

Decomposição de álgebras

Usamos técnicas topológicas para decompor e classificar algumas álgebras sobre um corpo k (todas supostas unitárias e comutativas).

3.1 Conjuntos algébricos

Dado $n \in \mathbb{N}$, há adjunção entre subconjuntos de k^n e ideais de $k[X_{[n]}] \coloneqq k[X_1, \ldots, X_n]$: $I(V \subseteq k^n) \coloneqq \{f \in k[X_{[n]}] \mid \forall_{x \in V} f(x) = 0\}$; $Z(J \subseteq k[X_{[n]}]) \coloneqq \{x \in k^n \mid \forall_{f \in J} f(x) = 0\}$; vale $IV \supseteq J \iff V \subseteq ZJ$. Logo, $IZIV = IV$, $ZIZJ = ZJ$, $I(\bigcup_i V_i) = \bigcap_i IV_i$, $Z(\bigcup_i J_i) = \bigcap_i ZJ_i$. Também, $Z\{1\} = \emptyset$, $Z(J_0 \cdot J_1) = ZJ_0 \cup ZJ_1$.

Definição 3.1.1. Chama-se de "topologia de Zariski" em k^n a topologia $\{ZJ \mid J \subseteq k[X_{[n]}]\}$. (Assim um "fechado" é um conjunto $V = ZIV$.) (Já os ideais da forma IV serão chamados de "saturados").

Definição 3.1.2. A "categoria das variedades afins" $k-\mathsf{Aff}$ tem como objetos os fechados $S \subseteq k^m$, $m \in \mathbb{N}$, e as setas $k-\mathsf{Aff}(S \subseteq k^m, T \subseteq k^n)$ são as funções $S \to T$ que são dadas por n polinômios em $k[X_{[m]}]$. (Alternativamente, as setas são as classes de equivalência $[(h_1, \ldots, h_n)]$, de n-tuplas de polinômios, módulo a relação de coincidirem nos pontos de S.)

Observação 3.1.3. Supõe-se k corpo infinito. Dadas k-álgebras A, B com ideais I, J, temos o homomorfismo sobrejetivo $(A \otimes B)/(I \otimes B + A \otimes J) \to A/I \otimes B/J$; mostremos ser injetivo. Supõe-se por absurdo que há, com número mínimo de parcelas, $\sum_{i=0}^{N} f_i \otimes g_i \notin I \otimes B + A \otimes J$ mas $\sum_{i=0}^{N} (f_i + I) \otimes (g_i + J) = 0$.

Se há dependência k-linear entre os $f_i + I$, digamos $f_j = \sum_{i \neq j} \lambda_i \cdot f_i + (x \in I)$, temos que $\sum_i f_i \otimes g_i = \sum_{i \neq j} f_i \otimes g_i + (\sum_{i \neq j} \lambda_i \cdot f_i + x) \otimes g_j = \sum_{i \neq j} f_i \otimes (g_i + \lambda_i \cdot g_j) + (x \in I) \otimes g_j$, logo o elemento $\sum_{i \neq j} f_i \otimes (g_i + \lambda_i \cdot g_j)$, com $< N + 1$ parcelas, está fora $I \otimes B + A \otimes J$ mas se anula na projeção a $A/I \otimes B/J$, absurdo.

Então, os $f_i + I$ são k-linearmente independentes; logo, cada $g_i + J = 0$, e $\sum_i f_i \otimes g_i \in A \otimes J$, contradição.

Portanto, se $S \subseteq k^m$ e $T \subseteq k^n$ estão em $k-\mathsf{Aff}$, vale $k[X_{[m]}]/IS \otimes k[Y_{[n]}]/IT \cong k[X_{[m]}, Y_{[n]}]/(IS \otimes k[Y_{[n]}] + k[X_{[m]}] \otimes IT)$, onde $Z(IS \otimes k[X_{[n]}] + k[X_{[m]}] \otimes IT) = ZIS \times ZIT = S \times T$. Este fechado $S \times T$ (na topologia de Zariski, não topologia-produto) é o produto na categoria $k-\mathsf{Aff}$.

Lema 3.1.4. *O functor* $k[\_] : (k-\mathsf{Aff})^\circ \to k-\mathsf{Alg}$*, dado por:*

$$k[S \subseteq k^m] \coloneqq \frac{k[X_{[m]}]}{IS},$$

$$k[\_]\left(S \subseteq k^m \overset{[(h_1,\ldots,h_n)]}{\to} T \subseteq k^n\right) \coloneqq \left[f \in k[X_{[n]}]\right] \mapsto \left[f(h_1,\ldots,h_n)\right],$$

é pleno e fiel.

Demonstração. Seja $\Phi : k[X_{[n]}]/IT \to k[X_{[m]}]/IS$ morfismo de k-álgebras. Então existem polinômios $r_1, \ldots, r_n \in k[X_{[m]}]$ tais que $\forall_{1\leq j\leq n} \Phi[X_j] = [r_j]$. Dado $[(h_1, \ldots, h_n)] \in k-\mathsf{Alg}(S^{\subseteq k^m}, T^{\subseteq k^n})$, temos

$$\begin{aligned} k[\_]\left[(h_1,\ldots,h_n)\right] = \Phi &\iff \forall_{[f\in k[X_{[n]}]]}[f(h_1,\ldots,h_n)] = \Phi[f] \\ &\iff \forall_{1\leq j\leq n}[X_j(h_1,\ldots,h_n)] = \Phi[X_j] \\ &\iff \forall_{1\leq j\leq n}[h_j] = [r_j] \\ &\iff [(h_1,\ldots,h_n)] = [(r_1,\ldots,r_n)]. \end{aligned}$$

□

Observação 3.1.5. O famoso Nullstellensatz (forte) de Hilbert diz que, se k é algebricamente fechado, os ideais saturados de $k[X_{[n]}]$ são precisamente os ideais radicais (isto é, ideais I tais que $I = \sqrt{I} \coloneqq \{x \mid \exists_{n\in\mathbb{N}} x^n \in I\}$). Há uma prova elementar por Oscar Zariski ("A new proof of Hilbert's Nullstellensatz", 1947), usando seu lema de Zariski (se $k \subseteq F$ é k-álgebra finitamente gerada e F é corpo, então $\dim_k F < \infty$). O Nullstellensatz implica que, se $k = \overline{k}$, e se A é uma k-álgebra finitamente gerada e reduzida (zero é o único nilpotente), sendo $A = k[X_{[n]}]/I$ (logo I radical), vale que $A \cong k[ZI]$.

3.1.1 Espaços topológicos noetherianos

Definição 3.1.6. Um espaço topológico X é dito "noetheriano" quando toda família não vazia de fechados de X admite pelo menos um fechado minimal.

Definição 3.1.7. Um espaço topológico X é dito "irredutível" quando não é união finita (≥ 0) de fechados próprios.

Teorema 3.1.8. *Todo espaço topológico noetheriano X admite quantidade finita de fechados irredutíveis maximais, e X se escreve como união deles.*

Demonstração. Prova-se primeiro que X é união finita de fechados irredutíveis. Supõe-se que não.

Seja $\mathcal{F}$ a família dos conjuntos fechados de X que não são uniões finitas de fechados irredutíveis; assim $\mathcal{F} \neq \emptyset$ porque $X \in \mathcal{F}$. Como X é noetheriano, $\mathcal{F}$ tem elemento minimal F. Em particular, F não é irredutível, nem vazio, logo existem F_1, $F_2 \subsetneq F$ fechados com $F = F_1 \cup F_2$. Pela minimalidade de F, vale $F_1, F_2 \notin \mathcal{F}$, logo F_1 e F_2 são uniões finitas de fechados irredutíveis, e $F = F_1 \cup F_2$ também, contradição.

Então temos decomposição $X = X_1 \cup \cdots \cup X_n$, em fechados irredutíveis distintos. Descartemos as parcelas X_i contidas noutras parcelas. Se Y é fechado irredutível qualquer, $Y = \bigcup_j (Y \cap X_j)$, logo há j com $Y = Y \cap X_j \subseteq X_j$. Desse modo: cada X_i será fechado irredutível maximal (senão X_i estará propriamente contido num fechado irredutível que por sua vez estará noutro X_j, e $X_i \subsetneq X_j$, absurdo); e todo fechado irredutível maximal de X é igual a um dos X_j. □

Exemplo 3.1.9. Se $I \subseteq k[X_{[m]}]$, os fechados de $Z(I)$ estão em bijeção com ideais saturados contendo $I \subseteq k[X_{[m]}]$, álgebra noetheriana, logo $Z(I)$ é espaço noetheriano.

Definição 3.1.10. Se A é um anel (comutativo unitário), seja seu "espectro" $\operatorname{Spec} A$ o conjunto dos ideais primos de A. Se $I \subseteq A$, define-se $Z(I) \coloneqq \{P \in \operatorname{Spec} A \mid P \supseteq I\}$. Então, $\{Z(I) \mid I \subseteq A\}$ é uma topologia de $\operatorname{Spec} A$. Como $\bigcap Z(I) = \sqrt{I}$, os fechados de $\operatorname{Spec} A$ estão em bijeção com os ideais radicais de A. Assim, se A é noetheriano, $\operatorname{Spec} A$ é noetheriano também.

Exemplo 3.1.11. Seja k corpo algebricamente fechado. Dada A uma k-álgebra finitamente gerada reduzida (zero é o único nilpotente), vale $A \cong k[X_{[m]}]/J$ para algum m e ideal radical J, que (pelo Nullstellensatz) é $J = I(S)$, $S \subseteq k^n$, logo $A \cong k[S]$.

Os ideais maximais M de A são com $A/M \cong k$ (lema de Zariski); logo os ideais maximais estão em bijeção com os homomorfismos $k[S] \cong A \to k \cong k[\bullet]$, que por sua vez estão em bijeção com os pontos de S.

Ainda mais, os fechados da topologia de S são os conjuntos $Z(I)$, saturados $I \subseteq A$ (isto é, ideais radicais $\sqrt{I} = \bigcap(ZI \subseteq \operatorname{Spec} A)$). Portanto, o subespaço dos ideais maximais de $\operatorname{Spec} A$ é homeomorfo a S.

Dada fatoração dum anel $A \cong A_1 \times \cdots \times A_n$, há elementos $e_i \coloneqq (0, \ldots, 1, \ldots, 0)$, com $\sum_i e_i = 1$ e $e_i \cdot e_j = [i = j] \cdot e_i$. Limitaremos o número de fatores n.

Definição 3.1.12. Um "sistema fundamental ortogonal de idempotentes" num anel A é uma sequência $(e_1, \ldots, e_n)$ de elementos de A satisfazendo $e_i \cdot e_j = [i = j] \cdot e_j$, $\sum_i e_i = 1$.

Lema 3.1.13. *Dada k-álgebra A, as partições de* $\operatorname{Spec} A$ *em dois fechados (abertos) são precisamente da forma* $\{Z\langle e\rangle, Z\langle 1-e\rangle\}$, *para idempotente e.*

Demonstração. Se e é idempotente, $Z\langle e\rangle \cup Z\langle 1-e\rangle = Z\langle e\cdot(1-e)\rangle = \operatorname{Spec} A$ e $Z\langle e\rangle \cap Z\langle 1-e\rangle = Z\langle e, 1-e\rangle = Z\langle 1\rangle = \emptyset$.

Por outro lado, se $\{ZI, ZJ\}$ é partição em dois fechados, vale $\operatorname{Spec} A = Z(I\cdot J)$ e $\emptyset = Z(I+J)$, logo $I\cdot J$ está no nilradical e $I+J=1$. Há $1 =: (a\in I)+(b\in J)$; há n com $(a\cdot b)^n = 0$; expanda $1 = (a+b)^{2n} = ua^n + vb^n$, $u, v \in A$; logo $ua^n = ua^n(ua^n+vb^n) = (ua^n)^2 + 0$, logo $e := ua^n$ é idempotente; vale $ZI \subseteq Z\langle e\rangle$, $ZJ \subseteq Z\langle 1-e\rangle$, e $ZI \cup ZJ = Z\langle e\rangle \cup Z\langle 1-e\rangle$ implica igualdades. □

Lema 3.1.14. *Dada k-álgebra noetheriana A, existe N tal que todo sistema fundamental ortogonal de idempotentes não nulos $(e_1, \ldots, e_n)$ de A tem no máximo N elementos.*

Demonstração. Seja $S := \operatorname{Spec} A$. Como A é noetheriano, S é noetheriano. Assim $S = \bigcup_{i=1}^{N} ZI_i$ para alguns ZI_i fechados irredutíveis maximais.

Seja agora $(e_1, \ldots, e_n)$ como no enunciado; $\{Z(\langle 1-e_j\rangle)\}_{j=1}^{n}$ é partição fechada de S (lema 3.1.13 repetido). Cada fechado irredutível ZI_i, $1 \le i \le N$ não pode intersectar simultaneamente dois fechados $Z\langle 1-e_j\rangle$, $1 \le j \le n$, dessa partição; logo cada $Z\langle 1-e_j\rangle$ é união de um ou mais dos ZI_i, logo $n \le N$. □

Corolário 3.1.15. *Toda k-álgebra noetheriana é produto finito $\prod_{i=1}^{n} A_i$ de k-álgebras, cada uma "conexa" (isto é, com exatamente dois idempotentes). Assim, os idempotentes de $A = \prod_{i=1}^{n} A_i$ são precisamente os elementos $(b_1, \ldots, b_n)$ para $b_i \in \{0, 1\}$, logo A tem precisamente 2^n idempotentes.*

Note que se adotarmos a ordem $e \preceq f \iff e = ef$ no conjunto de idempotentes, os elementos minimais $\neq 0$ de $A = \prod_{i=1}^{n} A_i$ serão os $(0, \ldots, 1, \ldots, 0)$, logo há precisamente n idempotentes minimais $\neq 0$ (também chamados idempotentes indecomponíveis), que estarão em bijeção com as componentes conexas do espectro.

Lema 3.1.16. *(a) Toda k-álgebra local de dimensão finita tem único ideal primo (que consequentemente é o seu nilradical e também o conjunto dos elementos não inversíveis).*

(b) Toda k-álgebra de dimensão finita e conexa é local.

(c) Toda k-álgebra de dimensão finita é produto finito de k-álgebras locais.

(d) Toda k-álgebra de dimensão finita e reduzida é produto finito de corpos.

Demonstração. (a) Seja A uma k-álgebra de dimensão finita. Se $P \subseteq A$ é ideal primo, A/P é domínio, e corpo também, logo P é ideal maximal. (De fato, se $[x] \in A/P$ é não divisor de zero, $[x]\cdot\_ : A/P \to A/P$ é mapa linear injetivo, logo bijetivo pois $\dim A/P < \infty$.)

Logo, se A é local, tem único ideal primo P. Seu nilradical será $\bigcap\{P\} = P$, e P, o único ideal maximal, é o conjunto dos não inversíveis.

(b) Seja B uma k-álgebra conexa de dimensão finita. Dados ideais primos distintos $P_1, \ldots, P_m$ (com $m \geq 1$) de B (que vimos que serão maximais porque $\dim B < \infty$), vale que $P_1 \cap \cdots \cap P_{m-1} \supsetneq P_1 \cap \cdots \cap P_m$; de fato, se valesse igualdade, então $P_1 \cap \cdots \cap P_{m-1} \subseteq P_m$, logo $P_1 \cdots P_{m-1} \subseteq P_m$, e como P_m é primo, há $1 \leq i \leq m-1$ com $P_i \subseteq P_m$, contradizendo maximalidade. Então B tem no máximo $\dim B + 1$ ideais primos.

Então $\operatorname{Spec} B$ é finito, cada ponto $\{P_i\}$ é fechado ZP_i, logo é uma componente conexa; como B é conexa, $\operatorname{Spec} B$ também é, logo tem único ideal primo.

(c) Pelo corolário 3.1.15, toda k-álgebra de dimensão finita é produto finito de k-álgebras conexas de dimensões finitas, que por (b) serão locais.

(d) O item (c) dá decomposição $A \cong \prod_i A_i$, e cada A_i não terá nilpotentes não nulos, logo seu o único ideal maximal (o nilradical) será trivial, e assim A_i será corpo. □

Lema 3.1.17. *Dado k corpo algebricamente fechado, dado $I \subseteq k[X_{[n]}]$ ideal (não necessariamente radical), a álgebra $k[X_{[n]}]/I$ é conexa se e só se $Z(I) \subseteq k^n$ é fechado conexo.*

Demonstração. Vale $k[X_{[n]}]/I$ conexa se e só se $\operatorname{Spec} \frac{k[X_{[n]}]}{I}$ (que é $\cong Z_{k[X_{[n]}]}(I)$) é conexo. Como $k = \overline{k}$, há (exemplo 3.1.11) mergulho $k^n \to \operatorname{Spec}(k[X_{[n]}])$, levando cada ponto $p \in k^n$ ao ideal maximal dos polinômios se anulando em p. Esse mergulho leva $Z(I) \subseteq k^n$ a um conjunto X tal que $\overline{X} = Z_{k[X_{[n]}]}(\bigcap X) = Z_{k[X_{[n]}]}(IZ_{k^n}I)$, que é $Z_{k[X_{[n]}]}(\sqrt{I}) = Z_{k[X_{[n]}]}(I)$ pelo Nullstellensatz. Assim, $k[X_{[n]}]/I$ é conexa sse $Z_{k[X_{[n]}]}(I) = \overline{X}$ é conexo, sse X é conexo (lema de topologia), sse $Z(I) \subseteq k^n$ é conexo. □

3.2 Álgebras separáveis

Definição 3.2.1. Uma k-álgebra de dimensão finita é dita "separável" quando é produto $\prod_i L_i$ onde cada $k \subseteq L_i$ é extensão separável finita (isto é, há $x_i \in L_i$ tal que $L_i = k(x_i)$ e o polinômio mínimo de x_i sobre k é separável).

Lema 3.2.2. *Dada k-álgebra A de dimensão finita, equivalem-se:*

(a) A é separável;

(b) $A \otimes k_s \cong k_s^{\dim_k A}$ (onde $k \subseteq k_s$ é extensão separável máxima);

(c) $A \otimes \overline{k} \cong \overline{k}^{\dim_k A}$ (onde $k \subseteq \overline{k}$ é fecho algébrico).

Demonstração. (a→b) Escrevendo-se $A \cong \prod_i k(x_i)$, onde x_i tem polinômio separável $f_i(x)$, vale $A \otimes k_s \cong \prod_i \left(\frac{k[x]}{(f_i(x))} \otimes k_s\right) \cong \prod_i \frac{k_s[x]}{(f_i(x))}$; como $f_i(x)$ é polinômio separável, fatora-se como $f_i(x) = \prod_{j=1}^{\deg f_i}(x - \alpha_{i,j}) \in k_s[x]$ onde os $\alpha_{i,j} \in k_s$, $1 \leq j \leq \deg f_i$, são

distintos. Assim,

$$A \otimes k_s \cong \prod_i \prod_{j=1}^{\deg f_i} \frac{k_s[x]}{(x-\alpha_{i,j})} \cong \prod_i k_s^{\deg f_i} \cong k_s^{\dim A}.$$

(b→c) Vale $A \otimes_k \overline{k} \cong A \otimes_k k_s \otimes_{k_s} \overline{k} \cong k_s^{\dim_k A} \otimes_{k_s} \overline{k} \cong \overline{k}^{\dim_k A}$.

(c→a) Escreva $A \cong \prod_i A_i$ onde cada A_i é álgebra local. Se um dos fatores A_i não é corpo, então o lema 3.1.16(a) diz que A_i tem nilpotente não nulo, logo A também, e $A \otimes \overline{k} \cong \overline{k}^{\dim_k A}$ também, absurdo.

Então cada fator A_i é corpo; basta mostrar que cada $k \subseteq A_i$ é extensão separável. Seja $a_i \in A_i$ elemento com polinômio mínimo f_i, e fatore-o no fecho algébrico, $f_i(x) = \prod_{i=1}^{n} (x-\alpha_i)^{e_i}$, onde os $\alpha_i \in \overline{k}$ são distintos. Assim,

$$A_i \otimes \overline{k} \supseteq k(a_i) \otimes \overline{k} \cong \frac{\overline{k}[x]}{(f_i(x))} \cong \prod_{i=1}^{n} \frac{\overline{k}[x]}{((x-\alpha_i)^{e_i})};$$

como $A_i \otimes \overline{k}$ está contido em $\overline{k}^{\dim A}$, não pode ter nilpotentes não nulos, assim cada expoente e_i é 1; logo a_i é separável. □

Observação 3.2.3. Se k é perfeito, uma k-álgebra é separável sse é de dimensão finita e reduzida.

Corolário 3.2.4. *Separabilidade de álgebras é preservada nas construções: tomar subálgebras, quocientes, produtos, produtos tensoriais e extensão de escalares.*

Demonstração. Se A é separável e se $B \subseteq A$ é subálgebra, vale $B \otimes \overline{k} \subseteq A \otimes \overline{k} \cong \overline{k}^{\dim A}$; assim $B \otimes \overline{k}$ é reduzida, e como $\overline{k}$ é perfeito, vale que $B \otimes \overline{k}$ é $\overline{k}$-separável (isto é $B \otimes \overline{k} \otimes_{\overline{k}} \overline{k} \cong \overline{k}^{\dim B}$), e assim B será k-separável.

Se A é separável e $B = A/I$ é quociente qualquer, vale $B \otimes \overline{k} = \frac{A}{I} \otimes \overline{k} = \frac{A \otimes \overline{k}}{I \otimes \overline{k}} \cong \frac{\overline{k}^{\dim A}}{I \otimes \overline{k}}$; o ideal $I \otimes \overline{k}$ é finitamente gerado (pois $\dim A < \infty$), logo $B \otimes \overline{k}$ é obtida por sucessivos quocientes de $\overline{k}^{\dim A}$ por ideais principais. E para cada $m \in \mathbb{N}$, dado $a \in \overline{k}^m$, o ideal gerado por a é precisamente $X := \{x \in \overline{k}^m \mid \forall_{1 \le i \le m}^{a_i = 0} x_i = 0\}$, logo $\overline{k}^m / \langle a \rangle$ é produto de fatores $\overline{k}$; então $B \otimes \overline{k}$ é produto de fatores $\overline{k}$, e B é separável.

Agora, se A_0 e A_1 são separáveis, $A_0 \times A_1$ e $A_0 \otimes A_1$ são separáveis também, porque: $(A_0 \times A_1) \otimes \overline{k} \cong \left(A_0 \otimes \overline{k}\right) \times \left(A_1 \otimes \overline{k}\right) \cong \overline{k}^{\dim A_0 + \dim A_1}$, $(A_0 \otimes_k A_1) \otimes \overline{k} \cong \left(A_0 \otimes \overline{k}\right) \otimes_{\overline{k}} \left(A_1 \otimes \overline{k}\right) \cong \overline{k}^{\dim A_0 \cdot \dim A_1}$.

Enfim, se $k \subseteq K$ é corpo, e se A é k-separável, vale que $A \otimes \overline{k} \cong \overline{k}^{\dim A}$, logo $(A \otimes_k K) \otimes_K \overline{K} \cong A \otimes_k \overline{K} \cong (A \otimes_k \overline{k}) \otimes_{\overline{k}} \overline{K} \cong \overline{K}^{\dim A}$, logo $A \otimes_k K$ é K-separável. □

3.2.1 Maior subálgebra separável

Lema 3.2.5. *Se A é uma k-álgebra finitamente gerada, existe maior subálgebra separável de A, que denotaremos $\pi_0(A)$.*

Demonstração. Se $B \subseteq A$ é subálgebra separável, temos que $k_s^{\dim B} \cong B \otimes k_s \subseteq A \otimes k_s$, assim $B \otimes k_s$ tem $\dim B$ idempotentes indecomponíveis; pelo corolário 3.1.15, a k_s-álgebra $A \otimes k_s$ (também finitamente gerada, logo noetheriana), tem número finito N de idempotentes, logo $\dim B \leq \log_2 N$.

Desse modo toda subálgebra separável de A tem dimensão no máximo $\log_2 N$, logo existe subálgebra separável maximal $B \subseteq A$. De fato B será a maior subálgebra separável, pois se $C \subseteq A$ é outra subálgebra separável, o produto $BC \subseteq A$ será separável também (sendo quociente de $B \otimes C$), e contém B, logo $B = BC \supseteq C$. □

Corolário 3.2.6. *Dada A uma k-álgebra de dimensão finita, $\pi_0 A = k$ sse A é local e não contém extensão separável $k \subsetneq L$ (esta segunda condição já vale se existir homomorfismo $A \to k$).*

Lema 3.2.7. *Sejam k-álgebras finitamente geradas A e B.*

(a) $\pi_0(A \times B) = \pi_0(A) \times \pi_0(B)$.

(b) Se $k \subseteq K$ é corpo, vale $\pi_0^K(A \otimes K) = \pi_0(A) \otimes K$, onde π_0^K denota a maior K-subálgebra K-separável.

(c) $\pi_0(A \otimes B) = \pi_0(A) \otimes \pi_0(B)$.

(d) $\dim_k \pi_0 A$ *é o número de componentes conexas de* $\operatorname{Spec}(A \otimes k_s)$.

Demonstração. (Parte de (Waterhouse, 1979)) Nos três itens, as contenções $\supseteq$ são claras, pois $\times$, $\otimes$ e extensão de escalares preservam separabilidade.

(a) Imagens de separáveis são separáveis, logo as duas projeções de $\pi_0(A \times B)$ são separáveis, logo contidas em $\pi_0(A)$ e $\pi_0(B)$, respectivamente, e $\pi_0(A \times B) \subseteq \pi_0(A) \times \pi_0(B)$.

(b) Basta provar $\infty > \dim_K \pi_0(A) \otimes K = \dim \pi_0(A) \geq \dim_K \pi_0^K(A \otimes K)$; tal propriedade denotemos $P(A, K)$. Como

$$\dim_K \pi_0^K(A \otimes K) = \dim_{\overline{K}} \pi_0^K(A \otimes K) \otimes \overline{K} \leq \dim_{\overline{K}} \pi_0^{\overline{K}}(A \otimes \overline{K}),$$

vale $P(A, \overline{K}) \implies P(A, K)$. Usamos $k \subseteq k_s \subseteq \overline{k} \subseteq \overline{K}$ para irmos por passos.

Vale $\pi_0^{k_s}(A \otimes k_s) \cong k_s^M$ para $M \coloneqq \dim_{k_s} \pi_0^{k_s}(A \otimes k_s)$. Há ação de $\mathcal{G} \coloneqq \operatorname{Aut}(k_s \supseteq k)$ em $A \otimes k_s$ dada por $\sigma \cdot (a \otimes \lambda) \coloneqq a \otimes \sigma\lambda$; assim, a subálgebra dos pontos fixos $(A \otimes k_s)^{\mathcal{G}}$ é $A \otimes 1$. Os elementos de $\mathcal{G}$ são automorfismos de anéis, logo permutam os idempotentes de k_s^M; podemos escrever $\sigma(\lambda \cdot e_i \in k_s^M) = \sigma(\lambda) \cdot e_{\sigma(i)}$. Logo, $\mathcal{G}$ age em

$\{1,\dots,M\}$, e seja $\{\mathcal{G}\cdot i_1,\dots,\mathcal{G}\cdot i_o\}$ o conjunto das órbitas. Logo todo ponto fixo de $\mathcal{G}$ em k_s^M é uma soma $\sum_{j=1}^{o}\sum_{i\in\mathcal{G}\cdot i_j}\lambda_i\cdot e_i$ tal que

$$\forall_{\sigma\in\mathcal{G}}\forall_{1\le j\le o}\sum_{i\in\mathcal{G}\cdot i_j}\sigma(\lambda_i)\cdot e_{\sigma(i)}=\sum_{i\in\mathcal{G}\cdot i_j}\lambda_i\cdot e_i,$$

isto é, $\forall_{\sigma\in\mathcal{G}}\forall_{1\le j\le o}\forall_{\tau i_j}\sigma(\lambda_{\tau i_j})=\lambda_{\sigma\tau i_j}$. Noutras palavras,

$$\begin{aligned}\left(k_s^M\right)^{\mathcal{G}}&=\left\{\sum_{j=1}^{o}\sum_{\tau i_j\in\mathcal{G}\cdot i_j}\tau(\lambda_{i_j})\cdot e_{\tau i_j}\mid\forall_{1\le j\le o}\forall_{\sigma\in\mathcal{G}}\sigma i_j=i_j\implies\sigma(\lambda_{i_j})=\lambda_{i_j}\right\}\\&=\left\{\sum_{j=1}^{o}\sum_{\tau i_j\in\mathcal{G}\cdot i_j}\tau(\lambda_{i_j})\cdot e_{\tau i_j}\mid\forall_{1\le j\le o}\lambda_{i_j}\in k_s^{S_{\mathcal{G}}i_j}\right\}\\&\cong\prod_{j=1}^{o}k_s^{S_{\mathcal{G}}i_j}.\end{aligned}$$

Vale $\dim_k(k_s^M)^{\mathcal{G}}=\sum_{j=1}^{o}|\frac{\mathcal{G}}{S_{\mathcal{G}}i_j}|=\sum_{j=1}^{o}|\mathcal{G}\cdot i_j|=M$ por resultados em ações de grupos finitos. (A ação de $\mathcal{G}$ se fatora por meio dum quociente finito, precisamente o grupo $\mathcal{G}'$ dos automorfismos do menor subcorpo de Galois incluindo as componentes segundas dos idempotentes de $\pi_0^{k_s}(A\otimes k_s)$, e $\mathcal{G}/S_{\mathcal{G}}i_j\cong\mathcal{G}'/S_{\mathcal{G}'}i_j$.) Cada fator $k_s^{S_{\mathcal{G}}i_j}$ é extensão separável, logo a álgebra $(k_s^M)^{\mathcal{G}}$ é separável, e por meio do isomorfismo $\pi_0^{k_s}(A\otimes k_s)\cong k_s^M$, é levada para dentro de $\pi_0((A\otimes k_s)^{\mathcal{G}})=\pi_0(A\otimes 1)$. Então,

$$\dim_{k_s}\pi_0^{k_s}(A\otimes k_s)=:M=\dim_k\left(k_s^M\right)^{\mathcal{G}}\le\dim_k\pi_0(A\otimes 1),\quad P(A,k_s).$$

Note

$$\begin{aligned}P(A\otimes k_s,\overline{k})&\iff\dim_{k_s}\pi_0^{k_s}(A\otimes k_s)\ge\dim_{\overline{k}}\pi_0^{\overline{k}}(A\otimes k_s\otimes_{k_s}\overline{k})\\&\implies\dim\pi_0A\ge\dim_{\overline{k}}\pi_0^{\overline{k}}(A\otimes\overline{k})\iff P(A,\overline{k})\end{aligned}$$

porque já $P(A,k_s)$. Logo, sem perda de generalidade (SPDG), $k=k_s$.

Se a característica é zero, $k_s=\overline{k}$ e $P(A,\overline{k})$. Se a característica é $p>0$, vale $\pi_0^{\overline{k}}(A\otimes\overline{k})\cong\overline{k}^M$ (isto é, tem $\overline{k}$-base de idempotentes), e se $e=\sum a\otimes\lambda$ é idempotente de $\pi_0^{\overline{k}}(A\otimes\overline{k})$, existe p^m tal que cada $\lambda^{p^m}\in k_s$, logo $e=e^{p^m}=\sum a^{p^m}\otimes\lambda^{p^m}\in A\otimes k_s$, e assim $\pi_0^{\overline{k}}(A\otimes\overline{k})\subseteq\pi_0^{k_s}(A\otimes k_s)\otimes\overline{k}$. Logo, $P(A,\overline{k})$.

Assim como antes, podemos supor $k=\overline{k}$, e queremos $P(A,\overline{K})$. Vale $\pi_0A=\prod_i\overline{k}e_i$, logo $A\cong\prod_i Ae_i$, pelo item (a)

$$\pi_0^{\overline{K}}(A\otimes\overline{K})=\prod_i\pi_0^{\overline{K}}(Ae_i\otimes\overline{K}),$$

e queremos provar $\pi_0^{\overline{K}}(Ae_i \otimes \overline{K}) = \pi_0(Ae_i) \otimes \overline{K} = \overline{K}e_i$. Para tal, basta que cada $Ae_i \otimes \overline{K}$ seja conexa. Escreva $Ae_i = \overline{k}[X_{[n]}]/I$, de modo que

$$Ae_i \otimes \overline{K} = \overline{K}[X_{[n]}]/I_{\overline{K}}.$$

Pelo lema 3.1.17, Ae_i conexa implica $Z(I) \subseteq \overline{k}^n$ conexo. Usando uma base de $\overline{K}$ sobre $\overline{k}$, pode-se ver que $Z_{\overline{K}^n}(I_{\overline{K}})$ é o fecho (em $\overline{K}^n$) de $Z(I) \subseteq \overline{k}^n \subseteq \overline{K}^n$, logo é conexo também. O mesmo lema implica $Ae_i \otimes \overline{K}$ ser conexa.

(c) Escreva $A = \prod_i A_i$ e $B = \prod_j B_j$, onde os fatores A_i e B_j são conexos. De (a), vale $\pi_0 A = \prod_i \pi_0 A_i$ e $\pi_0 B = \prod_j \pi_0 B_j$. Logo, $A \otimes B \cong \prod_{i,j} A_i \otimes B_j$, e nesse isomorfismo $\pi_0 A \otimes \pi_0 B \cong \prod_{i,j} \pi_0 A_i \otimes \pi_0 B_j$ e $\pi_0(A \otimes B) \cong \prod_{i,j} \pi_0(A_i \otimes B_j)$.

Logo, basta provar $\pi_0(A_i \otimes B_j) = \pi_0 A_i \otimes \pi_0 B_j$, isto é, que as dimensões coincidem. Pelo item (b), vale $\pi_0^{\overline{k}}(A_i \otimes \overline{k}) = \pi_0 A_i \otimes \overline{k}$, logo basta provar que

$$\dim_{\overline{k}} \pi_0^{\overline{k}}((A_i \otimes \overline{k}) \otimes_{\overline{k}} (B_j \otimes \overline{k})) = \dim_{\overline{k}} \pi_0^{\overline{k}}(A_i \otimes \overline{k}) \otimes \pi_0^{\overline{k}}(B_j \otimes \overline{k}).$$

Assim, sem perda de generalidade, $k = \overline{k}$ e A, B são conexas; queremos $A \otimes B$ conexa também; de fato, sendo $A = k[X_{[m]}]/I$ e $B = k[Y_{[n]}]/J$, vale $A \otimes B \cong k[X_{[m]}, Y_{[n]}]/(I \cdot k[Y_{[n]}] + k[X_{[m]}] \cdot J)$; lembrar (observação 3.1.3)

$$Z(I \cdot k[Y_{[n]}] + k[X_{[m]}] \cdot J) = Z(I) \times Z(J).$$

Como $Z(I)$ e $Z(J)$ são conexos (lema 3.1.17), $Z(I) \times Z(J)$ (não a topologia-produto) é conexo também: se $(a, b), (a', b') \in Z(I) \times Z(J)$, $\{a\} \times Z(J)$ é conexo, logo $(a, b), (a, b')$ estão na mesma componente conexa, e similarmente $(a, b'), (a', b')$. Portanto, $A \otimes B$ é conexa.

(d) $\dim_k \pi_0 A = \dim_{k_s}(\pi_0 A \otimes k_s) = \dim_{k_s}(\pi_0(A \otimes k_s))$ onde $\pi_0(A \otimes k_s) \cong k_s^M$; há M idempotentes indecomponíveis em $\pi_0(A \otimes k_s)$; e o número de componentes conexas de $\mathrm{Spec}(A \otimes k_s)$ é o número de idempotentes indecomponíveis em $A \otimes k_s$, que é M também, porque todo idempotente e está numa subálgebra separável $k_s 1 + k_s e$. □

Capítulo 4

Esquemas-grupos afins

Há três conceitos, variedades algébricas afins $\subseteq$ esquemas afins $\subseteq$ esquemas, estudados na geometria algébrica. Aqui tratamos do segundo, apesar das aplicações serem mais no primeiro.

Referências: (Waterhouse, 1979) e (Milne, 2015).

4.1 Esquemas afins

Definição 4.1.1. Um "esquema afim" (sobre k) consiste dum functor $F : k{-}\mathsf{Alg} \to \mathsf{Conj}$ e duma transformação natural $\hom(A, \_) \cong F$ para alguma A (que se chama "álgebra representante").

Um esquema afim é dito finito (resp., algébrico, de ordem $= n$), quando sua álgebra A é de dimensão finita (resp., finitamente gerada, de dimensão $= n$).

Pelo lema de Yoneda, $(\hom(A, \_) \implies \hom(B, \_)) \cong \hom(B, A)$, logo a "categoria dos esquemas afins" é $(k{-}\mathsf{Alg})^\circ$.

Definição 4.1.2. Um "esquema afim em grupos" (ou esquema-grupo afim) é um objeto-grupo na "categoria dos esquemas afins" . (Isto é, consiste dum esquema afim F e de transformações naturais $1 \implies F$, $F \implies F$ e $F \times F \implies F$ satisfazendo etc).

Vale $\mathsf{Grp}((k{-}\mathsf{Alg})^\circ) \cong (\mathsf{CoGrp}k{-}\mathsf{Alg})^\circ$, onde $\mathsf{CoGrp}\mathcal{A}$ é a categoria dos "objetos-cogrupos" de $\mathcal{A}$ (definem-se quase como os objetos-grupos, mas trocando o produto $\times$ pelo coproduto $\otimes$, e invertendo as setas; isto é, $\epsilon : A \to k$, $S : A \to A$ e $\Delta : A \otimes A \to A$, chamadas respectivamente counidade, coinverso e comultiplicação, satisfazendo $\langle\langle\rangle \circ \epsilon, 1\rangle \circ \Delta = 1 = \langle 1, \langle\rangle \circ \epsilon\rangle \circ \Delta$, $\langle 1, S\rangle \circ \Delta = \langle\rangle \circ \epsilon = \langle S, 1\rangle \circ \Delta$ e $(\Delta \otimes 1) \circ \Delta = (1 \otimes \Delta) \circ \Delta$ [coassociatividade]). Lembrar a notação $\langle f, g\rangle(a \otimes b) \coloneqq fa \cdot gb$.

Definição 4.1.3. Uma "álgebra de Hopf" é um objeto de $\mathsf{CoGrp}k{-}\mathsf{Alg}$. Uma álgebra de Hopf é "cocomutativa" quando seu esquema-grupo afim associado é abeliano.

Observação 4.1.4. Assim como vimos para objetos-grupos, os mapas de Hopf são os homomorfismos de álgebras $f : A \to B$ satisfazendo $(f \otimes f) \circ \Delta_A = \Delta_B \circ f$, condição que implica $\epsilon_A = \epsilon_B \circ f$ e $f \circ S_A = S_B \circ f$. Um mapa de Hopf que seja bijetivo será um isomorfismo de Hopf. Também, existem functores de extensões de escalares $\mathsf{CoGrp}k{-}\mathsf{Alg} \to \mathsf{CoGrp}K{-}\mathsf{Alg}$, $k \subseteq K$, $A \mapsto A \otimes K$ (mas não de restrições de escalares, por causa da counidade). E uma álgebra de Hopf é cocomutativa quando $\tau \circ \Delta = \Delta$ (onde $\tau(a \otimes b) \coloneqq b \otimes a$). E há a álgebra de Hopf trivial k.

Observação 4.1.5. Se $\eta : F \cong \hom(A, \_)$ onde F tem operações de grupos naturais, queremos descrever as operações de Hopf de A. O neutro $u : 1 \implies F$ passa a $\hom(k, \_) \implies \hom(A, \_)$, que pelo lema de Yoneda é $\hom(A, k)$. Logo $\epsilon \coloneqq \eta_k(u_k \bullet)$. O inverso $i : F \implies F$ passa a $\hom(A, \_) \implies \hom(A, \_)$, que é $\hom(A, A)$. Logo $S \coloneqq \eta_A(i(\eta_A^{-1}(1_A)))$. O produto $(\cdot) : F \times F \implies F$ passa a $\hom(A, \_) \times \hom(A, \_) \cong \hom(A \otimes A, \_) \implies \hom(A, \_)$. Logo sendo $\iota_0(a) = a \otimes 1$ e $\iota_1(a) = 1 \otimes a$, vale

$$\Delta \coloneqq \eta_{A \otimes A} \left(\eta_{A \otimes A}^{-1}(\iota_0) \cdot \eta_{A \otimes A}^{-1}(\iota_1) \right).$$

Exemplo 4.1.6. Esquemas-grupos básicos: $\boldsymbol{G_m}(R) \coloneqq R^\times$ (grupo na multiplicação); $\underline{\mu}_n(R) \coloneqq \{x \in R \mid x^n = 1\}$ (na multiplicação); $\boldsymbol{G_a}(R) \coloneqq R$ (grupo na adição); se p é a característica do corpo, $\underline{\alpha}_{p^n}(R) \coloneqq \{x \in R \mid x^{p^n} = 0\}$ (na adição); $\mathrm{GL}_m(R) \coloneqq$ matrizes inversíveis $R^{m \times m}$.

Suas álgebras de Hopf: $k[X, X^{-1}]$, com $\epsilon X = 1$, $SX = X^{-1}$, $\Delta X = X \otimes X$; $k[X]/(X^n - 1)$, mesmas operações; $k[X]$, com $\epsilon X = 0$, $SX = -X$, $\Delta X = X \otimes 1 + 1 \otimes X$; $k[X]/(X^{p^n})$, mesmas operações; $A_{\mathrm{GL}_m} \coloneqq k[X_{i,j}]_{i,j=1}^m[Y]/(\det(X_{\bullet\bullet}) \cdot Y - 1)$, $\epsilon X_{i,j} = [i = j]$, $\Delta X_{i,j} = \sum_l X_{i,l} \otimes X_{l,j}$, $SX_{i,j} = ((X_{\bullet\bullet})^{-1})_{i,j}$, usando a fórmula de Cramer.

Exemplo 4.1.7. Se k é corpo infinito e $(S \subseteq k^n) \in \mathsf{Grp}(k{-}\mathsf{Aff})$, então $k[S]$ tem estrutura de álgebra de Hopf: $\epsilon(f(x)) = f(1_S)$; $S(f(x)) = f(x^{-1})$ (onde x^{-1} é polinômio nas $x_1, \ldots, x_n$); $\Delta(f(x)) = f(m(x_1 \otimes 1, \ldots, x_n \otimes 1, 1 \otimes x_1, \ldots, 1 \otimes x_n))$ (onde m é o produto do grupo, polinômio de $2n$ variáveis). Reciprocamente, como $k[\_]$ é functor pleno fiel, e $k[S] \otimes k[S] \cong k[S \times S]$, toda estrutura de Hopf em $k[S]$ é dessa forma.

Fato 4.1.8. *A "categoria dos esquemas-grupos afins" tem todos os limites pequenos (sendo os mesmos que os limites de functores).*

Demonstração. Limite de representáveis é representável (com $\lim \hom(F(\_),) \cong \hom(\operatorname{co\lim} F(\_))$), e as operações de grupos passam ao limite. □

Observação 4.1.9. Em particular, os colimites de álgebras de Hopf são dados pelos mesmos colimites de álgebras. A categoria $\mathsf{CoAb}k{-}\mathsf{Alg}$ (álgebras de Hopf cocomutativas) também tem os mesmos colimites.

Lema 4.1.10. *Todo álgebra de Hopf A é união direcionada de subespaços V de dimensões finitas com $\Delta V \subseteq A \otimes V$.*

Demonstração. Se $\Delta V_i \subseteq A \otimes V_i$, então $\Delta(\sum_i V_i) \subseteq A \otimes \sum_i V_i$. Então basta provar que cada $v \in A$ está num subespaço V, $\dim < \infty$, com $\Delta V \subseteq A \otimes V$. Seja (a_i) base de A; escreva $\Delta a_i =: \sum_{j,l} \lambda_{i,j,l} \cdot a_j \otimes a_l$, para únicos $\lambda_{j,l} \in k$. Escreva $\Delta v = \sum_{i \in \mathcal{I}} a_i \otimes v_i$, para únicos $v_i \in A$, i num subconjunto finito $\mathcal{I}$. Logo, $(\Delta \otimes 1)(\Delta v) = (1 \otimes \Delta)(\Delta v)$, isto é, $\sum_i \Delta a_i \otimes v_i = \sum_{i,j,l} \lambda_{i,j,l} \cdot a_j \otimes a_l \otimes v_i = \sum_j a_j \otimes \Delta v_j$, então cada $\Delta v_j = \sum_{i,l} \lambda_{i,j,l} \cdot a_l \otimes v_i$. Use $V := \sum_{i \in \mathcal{I}} k \cdot v_i$, com $v = \langle \epsilon, 1 \rangle (\Delta v) = \sum_i \epsilon a_i \cdot v_i \in V$. □

Fato 4.1.11. *Toda álgebra de Hopf é união direcionada de subálgebras de Hopf que são finitamente geradas como álgebras.*

Demonstração. Pelo lema 4.1.10, cada sistema finito de elementos está contido num subespaço V, $\dim V < \infty$, com $\Delta V \subseteq A \otimes V$. Seja $(v_i)_{i<N}$ base de V; escreva $\Delta v_i = \sum_{j<N} a_{i,j} \otimes v_j$; logo, $(\Delta \otimes 1)(\Delta v_i) = (1 \otimes \Delta)(\Delta v_i)$, então $\Delta a_{i,j} = \sum_{l<N} a_{i,l} \otimes a_{l,j}$, i, $j < N$; logo $(a_{i,j}, Sa_{i,j})_{i,j<N}$ gera subálgebra de Hopf finitamente gerada, incluindo os $v_i = \sum_j a_{i,j} \cdot \epsilon v_j$, logo contendo V. □

Será escrito [finitamente gerada] para as hipóteses que o fato acima prove redundantes.

Definição 4.1.12. Um "quociente de Hopf" de A é uma álgebra de Hopf A/I tal que $\pi : A \to A/I$ seja homomorfismo de Hopf. (A projeção $\pi : A \to A/I$ corresponde a um mapa de esquemas-grupos injetivo, que é chamado de "continência de subgrupo fechado").

Fato 4.1.13. *Se A/I é um quociente de Hopf de A, vale $\epsilon I = 0$, $SI \subseteq I$ e $\Delta I \subseteq I \otimes A + A \otimes I$. (Chama-se I de ideal de Hopf).*

Demonstração. Como $\pi : A \to A/I$ é homomorfismo de Hopf, $\Delta : A \to A \otimes A$ induz a operação de Hopf $A/I \to A/I \otimes A/I \cong (A \otimes A)/(A \otimes I + I \otimes A)$, que para estar bem definida exige $\Delta I \subseteq A \otimes I + I \otimes A$. Outros mais fáceis. □

Lema 4.1.14. *Se A é uma álgebra de Hopf finitamente gerada, então há $m \in \mathbb{N}$ e quociente de Hopf $A_{\mathrm{GL}_m} \to A$.*

Demonstração. Pelo lema 4.1.10, há subespaço V, $\dim V < \infty$, com $\Delta V \subseteq A \otimes V$, e contendo um sistema finito de geradores para A. Seja $(v_i)_{i<m}$ base de V, escreva $\Delta v_i = \sum_j a_{i,j} \otimes v_j$; logo, $\Delta a_{i,j} = \sum_l a_{i,l} \otimes a_{l,j}$; também, $v_i = \langle \epsilon, 1 \rangle (\Delta v_i) = \sum_j \epsilon a_{i,j} \cdot v_j$, então $\epsilon a_{i,j} = [i = j]$. Também, $\sum_l a_{i,l} \cdot Sa_{l,j} = \langle 1, S \rangle (\Delta a_{i,j}) = \epsilon a_{i,j} = [i = j]$; isto é, a matriz $(a_{i,j})_{i,j<m}$ é inversível. Logo, sendo $\phi : A_{\mathrm{GL}_m} \to A$, $\phi X_{i,j} := a_{i,j}$, ϕ é homomorfismo de Hopf, sobrejetivo porque os geradores de A são $v_i = \sum_j a_{i,j} \cdot \epsilon v_j$. □

Observação 4.1.15. Por vezes é mais fácil usar esquemas-grupos. Por exemplo, dado mapa de Hopf $A \xrightarrow{f} A'$, associado a mapa $G \xleftarrow{F} G'$ de esquemas-grupos afins, temos $G' \times_G G' \xrightarrow{\sim} G' \times \operatorname{nuc} F$ (onde $(G' \times_G G')(R) := \{(g_0, g_1) \mid F_R g_0 = F_R g_1\}$, produto-fibrado) por $(g_0, g_1) \mapsto (g_0, g_0^{-1} \cdot g_1)$; logo há isomorfismo de Hopf $A' \otimes_A A \xleftarrow{\sim} A' \otimes_k \frac{A'}{f(\operatorname{nuc} \epsilon_A) \cdot A'}$ dado por $a_0 \otimes_k [a_1] \mapsto (a_0 \otimes_A 1) \cdot (S \otimes_A 1)(\Delta a_1)$.

4.1.1 Comódulos

Definição 4.1.16. Dada A uma álgebra de Hopf, um "comódulo" (esquerdo) sobre A consiste de linear $\rho : V \to A \otimes V$ tal que: $\langle \epsilon, 1 \rangle \circ \rho = 1_V$ (coneutro); $(1 \otimes \rho) \circ \rho = (\Delta \otimes 1) \circ \rho$ (coassociatividade).

Observação 4.1.17. Há a categoria dos A-comódulos. Há somas de comódulos, $V \oplus V' \to A \otimes (V \oplus V')$.

Há produtos tensoriais, $\tau : V \otimes V' \to A \otimes (V \otimes V')$, dado por $V \otimes V' \to (A \otimes V) \otimes (A \otimes V') \xrightarrow{P} A \otimes (V \otimes V')$, onde $P((a \otimes v) \otimes (a' \otimes v')) \coloneqq (a \cdot a') \otimes (v \otimes v')$. Prova das propriedades: chamamos os comódulos de $\rho : V \to A \otimes V$ e $\sigma : W \to A \otimes W$; sejam $v_\bullet, w_\bullet$ bases fixas, escrevemos $\rho v_i \coloneqq \sum_i a_{i,j} \otimes v_j$ e $\sigma w_I \coloneqq \sum_J b_{I,J} \otimes w_J$, então

$$\langle \epsilon, 1 \rangle (\tau(v_i \otimes w_I)) = \langle \epsilon, 1 \rangle \sum_{j,J} (a_{i,j} \cdot b_{I,J}) \otimes (v_j \otimes w_J) = \sum_{j,J} 1 \otimes \epsilon a_{i,j} \cdot v_j \otimes \epsilon b_{I,J} \cdot w_J = 1 \otimes v_i \otimes w_I,$$

$$\begin{aligned}(1 \otimes \tau)(\tau(v_i \otimes w_I)) &= \sum_{j,J} (a_{i,j} \cdot b_{I,J}) \otimes \tau(v_j \otimes w_J) = \sum_{j,J,k,K} (a_{i,j} \cdot b_{I,J}) \otimes (a_{j,k} \cdot b_{J,K}) \otimes (v_k \otimes v_K) \\ &= \sum_{j,J} (\Delta a_{i,k} \cdot \Delta b_{I,K}) \otimes (v_k \otimes v_K) = (\Delta \otimes 1)(\tau(v_i \otimes w_I))\end{aligned}$$

Se $V \cong k^{\times N}$, sendo $\rho e_i \coloneqq \sum_j a_{i,j} \otimes e_j$, temos como nas provas do fato 4.1.11 e 4.1.14: $\epsilon a_{i,j} = [i = j]$; $\Delta a_{i,j} = \sum_l a_{i,l} \otimes a_{l,j}$; $\sum_l a_{i,l} \cdot S a_{l,j} = [i = j]$; e $\det(a_{\bullet\bullet})$ é inversível. Então, temos mapa de Hopf $\phi_\rho : A_{\mathrm{GL}_N} \to A$ levando $X_{i,j} \mapsto a_{i,j}$. Logo um comódulo finito é dado por um $G \to \mathrm{GL}_N$, isto é, uma ação natural $G(R) \times R^{\times N} \to R^{\times N}$ linear na segunda componente.

4.2 Alguns esquemas-grupos afins específicos

Definição 4.2.1. Dado M grupo abeliano, define-se estrutura de Hopf na álgebra de grupo $k[M]$: $\epsilon(e_m) \coloneqq 1$; $S(e_m) \coloneqq e_{m^{-1}}$; $\Delta(e_m) \coloneqq e_m \otimes e_m$. (Chama-se álgebra de Hopf para "esquema-grupo afim diagonalizável").

Fato 4.2.2. *Seja A uma k-álgebra de Hopf. Denote $\mathcal{A} \coloneqq \{a \in A^\times \mid \Delta a = a \otimes a\}$. Então:*

1. *$\mathcal{A}$ é linearmente independente;*
2. *se $\mathcal{A}$ gera A como espaço vetorial, então $A \cong k[\mathcal{A}]$;*
3. *se $A = k[M]$, então $\mathcal{A} = \{e_m \mid m \in M\}$;*
4. *$k[\_] : \mathsf{Ab} \to \mathsf{CoGrp}k\mathsf{-Alg}$ é um functor pleno e fiel.*

Demonstração. (1) Prova-se por indução em $n \in \mathbb{N}$ que se $a_1, \dots, a_n \in \mathcal{A}$ são distintos são linearmente independentes. Caso $n = 0$, trivial. Para $n \geq 1$, supõe-se por absurdo que $a_n = \sum_{i<n} \lambda_i a_i$; logo

$$a_n \otimes a_n = \sum_{i,j<n} \lambda_i \lambda_j a_i \otimes a_j, \quad a_n \otimes a_n = \Delta a_n = \sum_{i<n} \lambda_i a_i \otimes a_i,$$

assim $\lambda_i \lambda_j = [i = j]\lambda_i$, o que dá (como k é corpo): no máximo um dos λ_i é não nulo; e o λ_i restante satisfaz $\lambda_i^2 = \lambda_i$, logo $\lambda_i \in \{0, 1\}$. Logo, $a_n = a_i$ para algum $i < n$, contradição.

(2) Assim $\mathcal{A}$ é base de A; é claramente grupo no produto. Assim temos isomorfismo de álgebras $k[\mathcal{A}] \cong A$; como $\Delta a = a \otimes a$ e $\Delta e_a = e_a \otimes e_a$ para cada $a \in \mathcal{A}$, esse isomorfismo é de Hopf também.

(3) Temos $\{e_m \mid m \in M\} \subseteq \mathcal{A}$, e igualdade vem de (1).

(4) Dado $\phi \in \mathsf{CoGrp}k\text{−}\mathsf{Alg}(k[M], k[N])$, vale $\Delta_{k[N]}(\phi e_a) = (\phi \otimes \phi)(\Delta_{k[M]} e_a) = \phi e_a \otimes \phi e_a$, assim de (3) $\phi e_a = e_{f(a)}$ para alguma f. Temos que $e_a \cdot e_b = e_{ab}$, logo $e_{fa} \cdot e_{fb} = e_{f(ab)}$, e $fa \cdot fb = f(ab)$, isto é, $f \in \mathsf{Ab}(M, N)$, e $\phi = k[\_](f)$. Então $k[\_]$ é functor pleno; e claramente fiel. □

Os elementos $a \in A^\times$ com $\Delta a = a \otimes a$ (equivalentemente, $a \in A$ com $\epsilon a = 1$ e $\Delta a = a \otimes a$) são ditos elementos "quase de grupo".

Definição 4.2.3. Dado Γ grupo finito, define-se estrutura de Hopf em k^Γ (que tem base $(e_g)_{g \in \Gamma}$) por: $\epsilon(e_g) = [g = 1]$; $S(e_g) = e_{g^{-1}}$; $\Delta(e_g) = \sum_{ab=g} e_a \otimes e_b$. (Chama-se de álgebra de Hopf para "esquema-grupo afim quase constante").

Fato 4.2.4. *Se X é um conjunto finito e k^X tem uma estrutura de Hopf $(k^X, \epsilon, S, \Delta)$, então X admite estrutura de grupo de modo que k^X seja álgebra de Hopf para quase constante.*

Demonstração. Os idempotentes de k^X são os elementos de $\{0, 1\}^{\times X}$. Então existem subconjuntos $\mathcal{S}x \subseteq X$ e $\mathcal{D}x \subseteq X \times X$ tais que (também idempotentes) $Se_x = \sum_{y \in \mathcal{S}x} e_y$ e $\Delta e_x = \sum_{(y,z) \in \mathcal{D}x} e_y \otimes e_z$. Como $Se_x \cdot Se_{x'} = 0$ e $\Delta e_x \cdot \Delta e_{x'} = 0$ (para $x \neq x'$), vale $\mathcal{S}x \cap \mathcal{S}x' = \emptyset$ e $\mathcal{D}x \cap \mathcal{D}x' = \emptyset$. Como $\sum_x Se_x = S1 = 1$ e $\sum_x \Delta e_x = 1$, vale $\bigcup_x \mathcal{S}x = X$ e $\bigcup_x \mathcal{D}x = X$. Então, $\{\mathcal{S}x \mid x \in X\}$ particiona X e $\{\mathcal{D}x \mid x \in X\}$ particiona $X \times X$: para cada $y \in X$ existe único $x \coloneqq y^{-1}$ com $y \in \mathcal{S}x$; e para cada $(y, z) \in X \times X$ existe único $x \coloneqq y * z$ com $(y, z) \in \mathcal{D}x$.

Vale $(\Delta \otimes 1)(\Delta e_x) = \sum_{y*z=x} \Delta e_y \otimes e_z = \sum_{y*z=x}^{y_0*y_1=y} e_{y_0} \otimes e_{y_1} \otimes e_z$, que é igual a $(1 \otimes \Delta)(\Delta e_x) = \sum_{y*z=x}^{z_0*z_1=z} e_y \otimes e_{z_0} \otimes e_{z_1}$; isto é, para $(a, b, c) \in X^{\times 3}$, vale que $(a*b)*c = x$ sse $a * (b * c) = x$, para cada x. Então, $*$ é associativa.

Também, existe único $u \in X$ com $\epsilon e_u = 1$; para $x \neq u$, vale $\epsilon e_x = 0$. Vale $e_x = \langle \epsilon, 1 \rangle(\Delta e_x) = \sum_{y*z=x} \epsilon e_y \cdot e_z = \sum_{u*z=x} e_z$, logo $u * x = x$; analogamente $x * u = x$. E $1 = \epsilon e_u = \langle 1, S \rangle(\Delta e_u) = \sum_{y*z=u}^{z_0^{-1}=z} e_y \cdot e_{z_0} = \sum_{y*y^{-1}=u} e_y$, logo $y * y^{-1} = u$ para cada y.

Portanto $*$ é operação de grupo em X, e $\Delta e_x = \sum_{y*z=x} e_y \otimes e_z$. □

4.3 Dualidade de Cartier

Definição 4.3.1. Dada k-álgebra de Hopf A cocomutativa de dimensão finita, define-se estrutura de k-álgebra comutativa no dual A^* por

$$1_{A^*} \coloneqq (\epsilon : A \to k),\ f \cdot g \coloneqq \langle f, g\rangle \circ \Delta,$$

e define-se estrutura de Hopf em A^* por

$$\epsilon_{A^*}(f) \coloneqq f(1),\ S_{A^*}(f) \coloneqq f \circ S,$$

$$\Delta_{A^*}(f) \coloneqq \Phi^{-1}\left(a \otimes b \mapsto f(a \cdot b)\right) = \Phi^{-1}\left(f \circ (\cdot)\right),$$

onde $\Phi : A^* \otimes A^* \to (A \otimes A)^*$ é dado por $\Phi(f \otimes g)(a \otimes b) = f(a) \cdot g(b)$, isto é, $\Phi(f \otimes g) = \langle f, g\rangle$, e Φ é isomorfismo pois $\dim A$ é finita. (Note que $A \supseteq Gk$ onde G é o esquema-grupo afim para A.)

Justifica-se (parcialmente) por que A^* é álgebra de Hopf. Sendo $\Delta_{A^*} f \coloneqq \sum g \otimes h$, vale $a \otimes b \mapsto f(a \cdot b)$ é igual a $a \otimes b \mapsto \sum g(a) \cdot h(b)$, logo

$$\begin{aligned}\langle \epsilon_{A^*}, 1\rangle \left(\Delta_{A^*} f\right)(c) &= \left(\langle \epsilon_{A^*}, 1\rangle \sum g \otimes h\right)(c) = \left(\sum g(1) \cdot h\right)(c) \\ &= \sum \langle g, h\rangle \left(1 \otimes c\right) = (f \circ (\cdot))(1 \otimes c) = f(c),\end{aligned}$$

$$\begin{aligned}\langle S_{A^*}, 1\rangle \left(\Delta_{A^*} f\right)(c) &= \left(\langle S_{A^*}, 1\rangle \sum g \otimes h\right)(c) = \left(\sum (g \circ S) \cdot_{A^*} h\right)(c) \\ &= \left(\sum \langle g \circ S, h\rangle \circ \Delta\right)(c) = \sum \langle g, h\rangle \left((S \otimes 1)(\Delta c)\right) \\ &= f\left(\langle S, 1\rangle \left(\Delta c\right)\right) = f(\epsilon c \cdot 1) = (\epsilon_{A^*}(f) \cdot 1_{A^*})(c),\end{aligned}$$

$$\begin{aligned}&\Phi_3((\Delta_{A^*} \otimes 1)(\Delta_{A^*} f))(a \otimes b \otimes c) = \Phi_3(\textstyle\sum \Delta_{A^*} g \otimes h)(a \otimes b \otimes c) = \sum g(a \cdot b) \cdot h(c) \\ &= f(a \cdot b \cdot c) = \textstyle\sum g(a) \cdot h(b \cdot c) = \Phi_3((1 \otimes \Delta_{A^*})(\Delta_{A^*} f))(a \otimes b \otimes c).\end{aligned}$$

Fato 4.3.2. *A dualidade de Cartier $A \mapsto A^*$ é uma equivalência da categoria das k-álgebras de Hopf cocomutativas de dimensões finitas com sua categoria oposta, e $A \cong A^{**}$ por meio de $a \mapsto (f \mapsto f(a))$.*

Observação 4.3.3. Se M é grupo finito comutativo, vale que $k[M]^* \cong k^M$.

Sendo $A \mapsto A^*$ uma antiequivalência, leva colimites em limites; e como nos esquemas-grupos afins abelianos o produto é o mesmo que o coproduto (ambos dados

por $(G \oplus H)(R) \coloneqq G(R) \oplus H(R)$), vale que $(A \otimes B)^* \cong A^* \otimes B^*$ como álgebras de Hopf.

Observação 4.3.4. Dado comódulo $\rho : V \to A \otimes V$, pode-se dar estrutura de A^*-módulo para V, por $A^* \otimes V \overset{1\otimes\rho}{\to} A^* \otimes A \otimes V \to V$. (Se a dimensão é infinita, A^* é só uma álgebra não necessariamente comutativa, não uma álgebra de Hopf). Também, se $U \subseteq V$ é um A^*-submódulo, mostra-se ser A-subcomódulo: sendo $(u_i)_{i\in B}$ base de U, estendida a base $(u_i)_{i\in C}$ de V, escreva $\rho u_i \coloneqq \sum_j a_{i,j} \otimes u_j$; a A^*-ação é $f \cdot u_i \coloneqq \langle f, 1\rangle(\rho u_i) = \sum_j f a_{i,j} \cdot u_j$; como $A^* \cdot U \subseteq U$, temos que $f a_{i,j} = 0$ para cada $i \in B$, $j \notin B$ e $f \in A^*$; então $a_{i,j} = 0$ para cada $i \in B$, $j \notin B$; e $\rho(V) \subseteq A \otimes V$.

4.3.1 Esquema de homomorfismos

Se $G : k\text{–}\mathsf{Alg} \to \mathsf{Conj}$ e R é k-álgebra, temos functor $G_R : R\text{–}\mathsf{Alg} \to \mathsf{Conj}$ dado por $G_R(A) \coloneqq G(A)$.

Definição 4.3.5. Dados esquemas-grupos afins G, H, define-se $\underline{\mathrm{Hom}}(G, H) : k\text{–}\mathsf{Alg} \to \mathsf{Conj}$ por:

$$\underline{\mathrm{Hom}}(G, H)(R) \coloneqq \mathsf{CoGrp}(R\text{–}\mathsf{Alg})\,(A_H \otimes R, A_G \otimes R) \cong \text{“}G_R \implies H_R\text{”}$$

Lema 4.3.6. *Se G é esquema-grupo afim abeliano finito, $\underline{\mathrm{Hom}}(G, \boldsymbol{G_m})$ é isomorfo ao dual de Cartier G^* (esquema afim associado a $(A_G)^*$).*

Demonstração. Vale

$$\begin{aligned}\underline{\mathrm{Hom}}(G, \boldsymbol{G_m})(R) &= \mathsf{CoGrp}(R\text{–}\mathsf{Alg})(k[X, X^{-1}] \otimes R, A_G \otimes R)\\ &\cong \mathsf{CoGrp}(k\text{–}\mathsf{Alg})(k[X, X^{-1}], A_G \otimes R),\end{aligned}$$

que é o conjunto dos elementos quase de grupo de $A \otimes R \coloneqq A_G \otimes R$. Já

$$\begin{aligned}G^*(R) &\cong k\text{–}\mathsf{Alg}(A^*, R)\\ &\subseteq k\text{–}\mathsf{Vect}(A^*, R) \cong k\text{–}\mathsf{Vect}(A^*, k) \otimes R \cong A \otimes R.\end{aligned}$$

Um elemento $e \coloneqq \sum a \otimes r \in A \otimes R$ associa-se a $\phi \in k\text{–}\mathsf{Vect}(A^*, R)$, $\phi(f) = \sum f(a) \cdot r$. As condições de ϕ ser homomorfismo de álgebras são:

$$\phi(\epsilon_A) = 1_R, \iff \sum \epsilon_A(a) \cdot r = 1_R;$$

$$\phi(f \cdot g) = \phi(f) \cdot \phi(g), \iff \sum \langle f, g\rangle\,(\Delta_A a) \cdot r = (\sum f(a) \cdot r) \cdot (\sum g(a) \cdot r)$$

Notar:

$$\epsilon_{A\otimes R}(e) = \sum \epsilon_A(a)\cdot r,$$

$$\begin{aligned}\langle f\otimes 1_R, g\otimes 1_R\rangle\,(\Delta_{A\otimes R}e) &= \sum \langle f,g\rangle\,(\Delta_A a)\cdot r,\\ \langle f\otimes 1_R, g\otimes 1_R\rangle\,(e\otimes_R e) &= (f\otimes 1_R)(e)\cdot(g\otimes 1_R)(e)\\ &= (\sum f(a)\cdot r)\cdot(\sum g(a)\cdot r).\end{aligned}$$

Logo ϕ é homomorfismo de álgebras sse $\sum a\otimes r$ é quase de grupo. □

4.4 Os fatores reduzido e conexo

Se A é álgebra de Hopf finitamente gerada, $\Delta(\pi_0 A)\subseteq \pi_0(A\otimes A) = \pi_0(A)\otimes \pi_0(A)$ (lema 3.2.7) e $S(\pi_0 A)\subseteq \pi_0 A$, logo $\pi_0 A\subseteq A$ é subálgebra de Hopf.

Seja B o conúcleo de $\pi_0 A\to A$, isto é, $B \coloneqq A/\langle \pi_0 A\cap \operatorname{nuc}\epsilon\rangle_A$. Se A é produto de conexas A_i, vale $\pi_0 A = \prod_i \pi_0 A_i$, $\operatorname{nuc}\epsilon = \prod_{i\neq 0} A_i$, onde sem perda de generalidade (SPDG) A_0 é o fator onde ϵ não se anula; logo $\pi_0 A\cap \operatorname{nuc}\epsilon \supseteq \prod_{i\neq 0} k$, logo $B = A_0$, conexa.

Fato 4.4.1. *Dado k corpo perfeito, dada A uma k-álgebra de Hopf finitamente gerada, temos decomposição $A\cong A_c[\otimes]A_r$ onde A_r é álgebra de Hopf reduzida (separável), A_l é álgebra de Hopf conexa, e $[\otimes]$ é o produto tensorial de álgebras mas com estrutura de Hopf de "produto semidireto". (Logo, se A é cocomutativa, $A\cong A_c\otimes A_r$, o produto tensorial usual).*

Demonstração. Seja $A_s \coloneqq \pi_0 A$. Seja $N\subseteq A$ o nilradical; como k é perfeito, A/N é separável, logo $A/N\otimes A/N$ também; logo o mapa $A\xrightarrow{\Delta} A\otimes A\to A/N\otimes A/N$ anula-se em N; então temos quociente de Hopf A/N.

O mapa $\alpha : A_s\to A\to A/N$ é injetivo porque A_s é reduzida, logo $A_s\cong \alpha(A_s)\subseteq \pi_0(A/N) = A/N$; vale $\dim_k A_s = \dim_{\overline{k}} \pi_0(A\otimes \overline{k})$, que é o número de componentes conexas de $\operatorname{Spec}(A\otimes\overline{k})$; também, $\dim_k A/N$ é o número de componentes conexas de $\operatorname{Spec}(A/N\otimes\overline{k}) = \operatorname{Spec}((A\otimes\overline{k})/N_{\overline{k}})$, homeomorfo a $\operatorname{Spec}(A\otimes\overline{k})$ porque $N_{\overline{k}}$ só tem nilpotentes; logo, $\dim_k A_s = \dim_k A/N$ e $A_s\cong A/N$.

A mônica $\pi_0 A\to A$ corresponde a épica $G\xrightarrow{f}\pi_0 G$; o conúcleo $A\to B = A/\langle \pi_0 A\cap\operatorname{nuc}\epsilon\rangle_A$ de $\pi_0 A\to A$ corresponde ao núcleo $G_0\xrightarrow{i} G$ de f; e a épica $A\to A/N\cong \pi_0 A$ corresponde a mônica $\pi_0 G\xrightarrow{s} G$ com $fs = \mathrm{id}$. Esta é precisamente a situação do produto semidireto, $G\cong G_0\rtimes \pi_0 G$.

□

Exemplo 4.4.2. Falha sem supor k perfeito. Por exemplo, sendo $k\coloneqq \mathbb{F}_2(X)$, tentaríamos definir $G(R)\coloneqq \{y\in R\mid y^2 = X\}$, mas este não é grupo, logo tentamos $G(R) = \{y\in R\mid y^4 = X\cdot y^2\}$ (na adição). Sua álgebra de Hopf é $A\coloneqq$

$k[Y]/(Y^2 \cdot (Y^2 - X)) \cong k[Y]/Y^2 \times k[\sqrt{X}]$, logo $\pi_0 A \cong k \times k$ (pois $k \subseteq k[\sqrt{X}]$ é inseparável); vale $A_0 \cong k[Y]/Y^2$, logo $A \ncong A_0 \otimes \pi_0 A$.

Observação 4.4.3. Dado mapa de Hopf $f : A \to B$ com $A \cong A_c[\otimes]A_r$ e $B \cong B_c[\otimes]B_r$ como acima, temos que f leva $\pi_0(A_c[\otimes]A_r) = k[\otimes]A_r$ a dentro de $\pi_0(B_c[\otimes]B_r) = k[\otimes]A_r$, de modo que haja único mapa $f_r : A_r \to B_r$ com $f(1[\otimes]a) = 1[\otimes]f_r(a)$; também,

$$A_c = \frac{A_c[\otimes]A_r}{\langle 1[\otimes]a\rangle_{a \in A_s \cap \operatorname{nuc}\epsilon}}, \; B_c = \frac{B_c[\otimes]B_r}{\langle 1[\otimes]b\rangle_{b \in B_s \cap \operatorname{nuc}\epsilon}},$$

e $a \in A_r \cap \operatorname{nuc}\epsilon \implies f(a) \in B_r \cap \operatorname{nuc}\epsilon$, logo f induz mapa $f_c : A_c \to B_c$, de modo que $f(a'[\otimes]1) = f_l(a')[\otimes]1$. Portanto, $f = f_s[\otimes]f_l$, isto é, a decomposição nos dois fatores é "functorial".

Se, ainda mais, A é cocomutativa e de dimensão finita, há dual de Cartier A^*, logo a decomposição $A \cong A_c \otimes A_r$ pode ser continuada $(A_x)^* \cong A_{x*c} \otimes A_{x*r}$, logo $A \cong \bigotimes_{x,y} A_{x*y*}$ em quatro fatores, onde A_{x*y*} é x de dual y, para $x, y =$ reduzida, conexa (= local em dimensão finita).

4.5 Em direção à categoria abeliana dos esquemas-grupos afins abelianos algébricos

Será muito importante provar que há a categoria abeliana dos esquemas-grupos afins abelianos, para manipularmos várias sequências exatas deles. O mais difícil será provar que nessa categoria toda mônica é núcleo e toda épica é conúcleo. Para tal, dado mapa de Hopf $f : A \to B$, serão investigados o sobrejetivo $A \to f(A)$ e a continência $f(A) \subseteq B$ de álgebras de Hopf.

4.5.1 Álgebras de Hopf reduzidas

Lema 4.5.1. *Dada A uma álgebra de Hopf, dado $f : A \to k$ linear, define-se a "translação" $T_f : A \to A$, $T_f := \langle 1, f\rangle \circ \Delta$. Então: (a) $T_\epsilon = 1$; (b) $\epsilon \circ T_f = f$; (c) se f é multiplicativo, $T_{f \circ S} = T_f^{-1}$; (d) se f satisfaz $f(a \cdot b) = \sum_i g_i(a) \cdot h_i(b)$ (lineares g_i, h_i), então $T_f(a \cdot b) = \sum_i T_{g_i}(a) \cdot T_{h_i}(b)$.*

Demonstração. (a) Hopf. (b) $\epsilon(T_f a) = f(\langle \epsilon, 1\rangle(\Delta a)) = f(a)$. (c) $T_{f\circ S} \circ T_f = \langle 1, f \circ S\rangle \circ \Delta \circ \langle 1, f\rangle \circ \Delta = \langle\langle 1, f \circ S\rangle, f\rangle \circ (\Delta \otimes 1) \circ \Delta = \langle 1, \langle f \circ S, f\rangle\rangle \circ (1 \otimes \Delta) \circ \Delta \overset{mult}{=} \langle 1, f \circ \langle 1, S\rangle\rangle \circ (1 \otimes \Delta) \circ \Delta = \langle 1, f\rangle \circ (1 \otimes \epsilon) \circ \Delta = \langle 1, f\rangle \circ (\_ \otimes 1) \overset{mult}{=} \mathrm{id}$. (d) De $\langle 1, f\rangle((x \otimes x') \cdot (y \otimes y')) = (x \cdot y) \cdot f(x' \cdot y') = \sum_i x \cdot g_i x' \cdot y \cdot h_i y' = \sum_i \langle 1, g_i\rangle(x \otimes x') \cdot \langle 1, h_i\rangle(y \otimes y')$. □

Teorema 4.5.2 (Cartier)**.** *Se k é corpo de característica zero e A é k-álgebra de Hopf [finitamente gerada], então A é reduzida.*

Demonstração. (De Waterhouse (1979) 11.4) Como $A \subseteq A \otimes \overline{k}$, supomos sem perda de generalidade (SPDG) que $k = \overline{k}$.

Denote $I \coloneqq \operatorname{nuc} \epsilon$; vale $A = k \oplus I$, logo A tem sistema finito de geradores $x_1, \ldots, x_m \in I$; seja $V = kx_1 + \cdots + kx_m$. Todo elemento de A escreve-se como polinômio nos x_i, logo $A = k + V + V^2 + \cdots$; também, $I^j \subseteq (V + V^2 + \cdots)^j \subseteq V^j + V^{j+1} + \cdots$. Reordenando os índices, SPDG, $[x_1], \ldots, [x_n]$ é base de I/I^2; denote $W = kx_1 + \cdots + kx_n$. Logo, $V \subseteq W + I^2 \subseteq I$; e $V^N \subseteq W^N + W^{N-1}I^2 + \cdots + I^{2N} \subseteq W^N + I^{N+1}$. Então, $I^N/I^{N+1} = (V^N + I^{N+1})/I^{N+1} \subseteq (W^N + I^{N+1})/I^{N+1}$; isto é, os $\left(\binom{n}{N}\right)$ produtos de N termos dentre $\{x_1, \ldots, x_n\}$ formam sistema gerador do espaço vetorial I^N/I^{N+1}.

Queremos mostrar $\dim_k I^N/I^{N+1} = \left(\binom{n}{N}\right)$. Para tal, supõe-se $\sum_{e_1+\cdots+e_n=N} \lambda_{(e_1,\ldots,e_n)} \cdot x_1^{e_1} \cdots x_n^{e_n} \in I^{N+1}$. Como temos uma situação similar ao anel polinomial $k[X_1, \ldots, X_n]$, definiremos n "derivadas parciais": define-se $d_i : A = k \oplus I \to k$ (como se fosse a derivada avaliada em zero) por $d_i(1) = 0$ e $d_i : I \to k$ dado por $I \to I/I^2 \xrightarrow{d_i'} k$ onde $d_i'[x_j] = [i = j]$, $1 \leq j \leq n$; define-se $D_i : A \to A$ por $D_i \coloneqq \langle 1, d_i \rangle \circ \Delta$.

Temos, $1 \leq i, j \leq n$, $\epsilon(D_i x_j) = \langle \epsilon, d_i \rangle (\Delta x_j) = d_i x_j = [i = j]$. Logo, $D_i x_j \equiv [i = j] \pmod{I}$.

Vale a regra de Leibnitz $d_i(a \cdot b) = d_i a \cdot \epsilon b + \epsilon a \cdot d_i b$: basta verificar nos quatro casos $a, b \in k, I$, fáceis. Assim, $D_i(a \cdot b) = D_i a \cdot b + a \cdot D_i b$. Em particular, $D_i(I^M) \subseteq M \cdot I^{M-1} \cdot D_i(I) \subseteq I^{M-1}$; e $D_i^j(I^M) \subseteq I^{M-j}$.

Para cada $e_1 + \cdots + e_n = N$,

$$\begin{aligned} D_i(x_1^{e_1} \cdots x_n^{e_n}) &= \sum_{j=1}^{n} e_j \cdot D_i x_j \cdot x_1^{e_1} \cdots x_j^{e_j - 1} \cdots x_n^{e_n} \\ &\in e_i \cdot x_1^{e_1} \cdots x_i^{e_i - 1} \cdots x_n^{e_n} + I^N, \\ D_i^{e_i}(x_1^{e_1} \cdots x_n^{e_n}) &\in e_i! x_1^{e_1} \cdots x_i^0 \cdots x_n^{e_n} + D_i^{e_i - 1}(I^N) + D_i^{e_i - 2}(I^{N-1}) + \cdots \\ &\subseteq e_i! x_1^{e_1} \cdots x_i^0 \cdots x_n^{e_n} + I^{N - e_i + 1}. \end{aligned}$$

Repetindo-se,

$$(D_1^{e_1} \cdots D_n^{e_n})(x_1^{e_1} \cdots x_n^{e_n}) \in e_1! \cdots e_n! \cdot 1 + I.$$

Também, se $f_1 + \cdots + f_n = N$ e $(f_1, \ldots, f_n) \neq (e_1, \ldots, e_n)$ há i com $e_i > f_i$, e como $D_i^{f_i+1}(x_1^{f_1} \cdots + x_n^{f_n}) \in I^{N - f_i}$, vale $(D_1^{e_1} \cdots D_n^{e_n})(x_1^{f_1} \cdots x_n^{f_n}) \in I$. Então, voltando à soma original,

$$(D_1^{e_1} \cdots D_n^{e_n}) \sum_{f_1 + \cdots + f_n = N} \lambda_{(f_1,\ldots,f_n)} x_1^{f_1} \cdots x_n^{f_n} \in \lambda_{(e_1,\ldots,e_n)} e_1! \cdots e_n! \cdot 1 + I$$

que também está em $(D_1^{e_1} \cdots D_n^{e_n})(I^{N+1}) \subseteq 0 + I$. Portanto, $\lambda_{(e_1,\ldots,e_n)} e_1! \cdots e_n! = 0$, e como a característica de k é zero, $\lambda_{(e_1,\ldots,e_n)} = 0$.

Temos então uma base para $I^N/I^{N+1} = (W^N + I^{N+1})/I^{N+1}$; logo, $\dim W^N =$

$\dim I^N/I^{N+1} = \left(\binom{n}{N}\right)$. Dado $a \in A$, temos então únicas escritas: $a = (a_0 \in k) + (a_{>0} \in I)$, e $a_{>0} = (a_1 \in W) + (a_{>1} \in I^2)$, $a_{>1} = (a_2 \in W^2) + (a_{>2} \in I^3)$, etc. Logo temos o mapa $\phi : A \to k \times W \times W^2 \times \cdots$, $\phi(a) \coloneqq (a_0, a_1, \ldots)$. Aplicando os isomorfismos $W^N \cong k[X_1, \ldots, X_n]_N$ (polinômios homogêneos de grau $= N$), $x_1^{e_1} \cdots x_n^{e_n} \leftrightarrow X_1^{e_1} \cdots X_n^{e_n}$, temos homomorfismo de álgebras $\psi : A \to k[[X_1, \ldots, X_n]]$.

Seja agora $a \in A$ com $a^2 = 0$ mas $a \neq 0$. Como $\{x \mid a \cdot x = 0\}$ é próprio, está contido num ideal maximal $\mathfrak{m}$. Pelo lema de Zariski, $A/\mathfrak{m} \cong k$; sendo $\pi : A \to A/\mathfrak{m} \cong k$, e $T_\pi : A \to A$ é isomorfismo de álgebras (não de Hopf) pelo lema anterior. De $\epsilon \circ T_\pi = \pi$, $T_\pi(\mathfrak{m}) \subseteq I$ (de fato iguais, pois maximais). Seja $b \coloneqq T_\pi(a)$; logo, $\{y \mid b \cdot y = 0\} \subseteq I$. Agora, de $a^2 = 0$ temos $\psi(b)^2 = 0$, $\psi(b) = 0$, isto é, $b = b_{>N}$ para cada N; logo, $b \in \bigcap_{N \geq 0} I^N$. (Aqui temos o teorema de interseção de Krull). Para cada $N \geq 0$ existe $P_N \in A[X_1, \ldots, X_m]_N$ com $b = P_N(x_1, \ldots, x_m)$. Como $A[X_1, \ldots, X_m]$ é Noetheriano, $\langle P_0, P_1, \ldots \rangle = \langle P_0, \ldots, P_{M-1} \rangle$ para algum M. Logo, $P_M = Q_0 \cdot P_0 + \cdots + Q_{M-1} \cdot P_{M-1}$; projetando nas componentes homogêneas de grau $= M$, SPDG, cada Q_i é homogêneo de grau $M - i$. Logo, $b = P_M(x_1, \ldots, x_m) = b \cdot (\sum_{i<M} Q_i(x_1, \ldots, x_m)) \in b \cdot I$. Logo, há $x \in I$ com $b \cdot (1 - x) = 0$, logo $1 - x \in I$, contradição. □

4.5.2 Álgebras de Hopf com ideais maximais nilpotentes

Lema 4.5.3. *Se $A \subseteq B$ são k-álgebras de Hopf e $\operatorname{nuc} \epsilon_A$ é ideal nilpotente, então B é A-livre.*

Demonstração. (De Milne (2015) 3j) Lembrar $B \otimes_A B \cong B \otimes_k \frac{B}{\langle \operatorname{nuc} \epsilon_A \rangle}$; seja $([b_i])_{i \in I}$ uma k-base de $\frac{B}{\langle \operatorname{nuc} \epsilon_A \rangle}$. Queremos mostrar $(b_i)_{i \in I}$ ser uma A-base de B.

Seja $C \coloneqq B/(\sum_i A \cdot b_i)$. Como $\frac{B}{\langle \operatorname{nuc} \epsilon_A \rangle} \subseteq \sum_i k \cdot [b_i]$, vale $B \subseteq B \cdot \operatorname{nuc} \epsilon_A + \sum_i k \cdot b_i$, logo $C \subseteq C \cdot \operatorname{nuc} \epsilon_A \subseteq C \cdot (\operatorname{nuc} \epsilon_A)^2 \subseteq \cdots \subseteq 0$. Então $B = \sum_i A \cdot b_i$.

Seja $\phi : B^{\oplus I} \to B \otimes_A B$ dado por $\phi(b \cdot e_i) \coloneqq b \otimes b_i$; seja $M \coloneqq \operatorname{nuc} \phi$. Dado $(v_i) \in M$, vale $\sum_i v_i \otimes b_i = 0 \in B \otimes_A B$, logo $\sum_i [v_i] \otimes [b_i] = 0 \in (\frac{B}{\langle \operatorname{nuc} \epsilon_A \rangle})^{\otimes 2}$, logo cada $v_i \in B \cdot \operatorname{nuc} \epsilon_A$; então, $M \subseteq (B \cdot \operatorname{nuc} \epsilon_A)^{\oplus I}$. E como $B \otimes_A B \cong B \otimes_k \frac{B}{\langle \operatorname{nuc} \epsilon_A \rangle}$ por meio de $b \otimes (\cdots) \mapsto (b \otimes 1) \cdot (\cdots)$, o B-módulo, com ação nos primeiros fatores, $B \otimes_A B$ é B-livre. Como $B = \sum_i A \cdot b_i$, vale $\phi(A^{\oplus I}) = A \otimes_A B$, logo $\phi(B^{\oplus I}) = B \otimes_A B$; existe N um submódulo de $B^{\oplus I}$ gerado por pré-imagens quaisquer duma base de $B \otimes_A B$. Então $B^{\oplus I} = M \oplus N$. Então, $M \subseteq \operatorname{nuc} \epsilon_A \cdot B^{\oplus I} = \operatorname{nuc} \epsilon_A \cdot M + \operatorname{nuc} \epsilon_A \cdot N \subseteq M \oplus N$, logo $M \subseteq \operatorname{nuc} \epsilon_A \cdot M \subseteq \cdots \subseteq 0$. Portanto, ϕ é injetivo, logo também a restrição $\phi : A^{\oplus I} \to A \otimes_A B$, então $(b_i)_{i \in I}$ é A-base de B. □

4.5.3 Fielmente planos

Definição 4.5.4. Um módulo M sobre R (sempre anel comutativo unitário) é dito "plano" (ou "chato", como no francês "plat") quando o produto tensorial $\_ \otimes M$:

$R-\mathsf{Mod} \to R-\mathsf{Mod}$ é functor exato. (Como já vimos $\_ \otimes M$ ser functor exato direito, M é módulo plano precisamente quando $\_ \otimes M$ leva continências $N_1 \subseteq N_2$ a injetivos $N_1 \otimes M \to N_2 \otimes M$.)

Definição 4.5.5. Um módulo M sobre R é dito "fielmente plano" quando é plano e: se $N_0 \subsetneq N$ é submódulo próprio de qualquer módulo, também $N_0 \otimes M \subsetneq N \otimes M$ é próprio. (Isto é, se $N/N_0 \neq 0$, então $M \otimes N/N_0 \neq 0$.)

Lema 4.5.6. *Seja A uma R-álgebra que seja fielmente plana (como um R-módulo). Então para cada R-módulo M, o equalizador dos mapas $M \otimes A \to M \otimes A \otimes A$, $m \otimes x \mapsto m \otimes x \otimes 1$ e $m \otimes x \mapsto m \otimes 1 \otimes x$, é precisamente $M \otimes 1$.*

Demonstração. Seja $N \subseteq M \otimes A$ o equalizador. Como $\_ \otimes A$ é functor exato, preserva os limites finitos, logo $N \otimes A$ é equalizador dos mapas associados $f_1 \otimes 1, f_2 \otimes 1 : M \otimes A \otimes A \to M \otimes A \otimes A \otimes A$. E dado $e \coloneqq \sum_i m_i \otimes x_i \otimes y_i \in N \otimes A$, vale $\sum_i m_i \otimes 1 \otimes x_i \otimes y_i = \sum_i m_i \otimes x_i \otimes 1 \otimes y_i$, e aplicando a multiplicação nos dois últimos fatores, vale $\sum_i m_i \otimes 1 \otimes x_i y_i = \sum_i m_i \otimes x_i \otimes y_i = e$; então $N \otimes A \subseteq M \otimes 1 \otimes A$; claramente $M \otimes 1 \subseteq N$, logo $M \otimes 1 \otimes A = N \otimes A$; de A ser fielmente plana, temos $M \otimes 1 = N$. □

Corolário 4.5.7. *Se $f : A \to B$ é epimorfismo de k-álgebras e B é A-fielmente plana, então f é sobrejetivo.*

Demonstração. Há a dupla-conúcleo (um colimite em $k-\mathsf{Alg}$) $A \xrightarrow{f} B \rightrightarrows B \otimes_A B$, onde os mapas $B \to B \otimes_A B$ são $x \mapsto x \otimes 1$ e $x \mapsto 1 \otimes x$. Como f é épica, vale $x \otimes 1 = 1 \otimes x \in B \otimes_A B$ para cada $x \in B$, que pelo lema anterior implica $x \in f(A) \cdot 1$. □

Lema 4.5.8. *(a) Se M/N é A-módulo plano, então $N \otimes_A P \to M \otimes_A P$ é sempre injetivo. (b) Se M/N é A-módulo plano, então M é A-plano sse N é A-plano. (c) Se M/N é A-plano, N é A-fielmente plano, então M é A-fielmente plano.*

Demonstração. (De Bourbaki (1985) I§2-3) (a) Seja presentação $0 \to P_R \xrightarrow{r} P_L \to P \to 0$ onde P_L é livre. Temos as linhas $N \otimes_A P_R \to M \otimes_A P_R \to M/N \otimes_A P_R$ e $N \otimes_A P_L \to M \otimes_A P_L \to M/N \otimes_A P_L$ e setas $(\cdots) \otimes_A P_R \xrightarrow{(\cdots) \otimes_A r} (\cdots) \otimes_A P_L$ entre elas. As duas linhas são exatas pois $\_ \otimes P_{(\cdots)}$ é sempre exato direito. Logo o lema da cobra (lema de homologia) dá a sequência exata $\operatorname{nuc}(M \otimes_A r) \to \operatorname{nuc}(M/N \otimes_A r) \to \operatorname{conuc}(N \otimes_A r) \to \operatorname{conuc}(M \otimes_A r)$; como M/N é plano e r é injetivo, vale que $\operatorname{nuc}(M/N \otimes_A r) = 0$; logo $\operatorname{conuc}(N \otimes_A r) \to \operatorname{conuc}(M \otimes_A r)$ é injetivo; e lembremos (exato direito) $\operatorname{conuc}((\cdots) \otimes_A r) = (\cdots) \otimes_A \operatorname{conuc} r$; portanto, $N \otimes_A P \to M \otimes_A P$ é injetivo.

(b) Dado A-injetivo $\phi : P \to Q$, temos as sequências exatas $N \otimes_A P \to M \otimes_A P \to M/N \otimes_A P$ e $N \otimes_A Q \to M \otimes_A Q \to M/N \otimes_A Q$ e setas $(\cdots) \otimes_A \phi$ entre elas. As setas $N \otimes_A (\cdots) \to M \otimes_A (\cdots)$ são injetivas por (a). Logo, $M \otimes_A P \to M \otimes_A Q$ injetivo implica $N \otimes_A P \to M \otimes_A P \to M \otimes_A Q$ injetivo, logo $N \otimes_A P \to N \otimes_A Q (\to M \otimes_A Q)$ também. Na outra direção, se $N \otimes_A P \to N \otimes_A Q$ é injetivo, lema de

homologia dá o mapa do meio $M \otimes_A P \to M \otimes_A Q$ injetivo (usando também que $M/N \otimes_A P \to M/N \otimes_A Q$ é injetivo porque M/N plano).

(c) De (b), temos M plano. E se $M \otimes_A P = 0$, temos do item (a) injetivo $0 \to N \otimes_A P \to M \otimes_A P = 0$, logo $N \otimes_A P = 0$, e $P = 0$. □

4.5.4 Álgebras de Hopf fielmente planas

Uma prova mais simples pode ser dada para álgebras de Hopf de dimensões finitas (usando 3.1.16(b)), porém precisaremos de algumas com dimensões infinitas. Usa-se Takeuchi (1972).

Definição 4.5.9. Dadas álgebras de Hopf $A \subseteq B$, um A–B-"comódulo" (à esquerda) é um comódulo $\rho : V \to B \otimes V$ junto a estrutura de A-módulo em V de modo que $\rho(a \cdot v) = \Delta a \cdot \rho v$ para cada $(a, v) \in A \times V$.

Lema 4.5.10. *Dado A–A-comódulo $\rho : V \to A \otimes_k V$, sendo $V' \coloneqq \{v \in V \mid \rho v = 1 \otimes v\}$, vale $A \otimes_k V' \cong V$ por meio da multiplicação; em particular, V é A-módulo livre.*

Demonstração. (De Sweedler (1969) 4.1.1) Denote $\tau(a \otimes b) \coloneqq b \otimes a$. Denote $P : V \to V$, $P \coloneqq \langle S, 1\rangle \circ \rho$. Mostra-se $P(V) \subseteq V'$: seja (v_i) base de V, escreva $\rho v_i = \sum_j a_{i,j} \otimes v_j$, então $Pv_i = \sum_j Sa_{i,j} \cdot v_j$, e $\rho(Pv_i) = \sum_j \Delta(Sa_{i,j}) \cdot \rho v_j = \sum_j (S \otimes S)(\tau(\Delta a_{i,j})) \cdot \rho v_j = \sum_{j,l,k} (Sa_{l,j} \otimes Sa_{i,l}) \cdot (a_{j,k} \otimes v_k) = \sum_{j,l,k} (Sa_{l,j} \cdot a_{j,k}) \otimes (Sa_{i,l} \cdot v_k) = \sum_{l,k} [l = k] \otimes (Sa_{i,l} \cdot v_k) = \sum_l 1 \otimes Sa_{i,l} \cdot v_l = 1 \otimes Pv_i$.

Notar $P(a \cdot v) = \langle S, 1\rangle(\rho(a \cdot v)) = \langle S, 1\rangle(\Delta a \cdot \rho v) = \epsilon a \cdot Pv$.

Definimos $\alpha : A \otimes V' \to V$ e $\beta : V \to A \otimes V'$: $\alpha(a \otimes v) \coloneqq a \cdot v$, $\beta v \coloneqq (1 \otimes P)(\rho v)$. Então: $\beta v_i = \sum_j a_{i,j} \otimes Pv_j$, $\alpha(\beta v_i) = \sum_j a_{i,j} \cdot Pv_j = \sum_{j,l} a_{i,j} \cdot Sa_{j,l} \cdot v_l = \sum_l [i = l] \cdot v_l = v_i$.

Notar $\beta(a \cdot v) = (1 \otimes P)(\Delta a \cdot \rho v) = (1 \otimes \epsilon)(\Delta a) \cdot (1 \otimes P)(\rho v) = (a \otimes 1) \cdot \beta(v)$. Então, sendo $u \in V'$, temos $\beta(\alpha(a \otimes u)) = \beta(a \cdot u) = (a \otimes 1) \cdot (1 \otimes P)(\rho u) = (a \otimes 1) \cdot (1 \otimes Pu) = (a \otimes 1) \cdot (1 \otimes \langle S, 1\rangle(\rho u)) = (a \otimes 1) \cdot (1 \otimes u) = a \otimes u$. □

Definição 4.5.11. Uma "coálgebra" é um objeto de $\mathsf{CoMon}(k\text{–}\mathsf{Vect}, \otimes)$ (isto é, um espaço vetorial V com lineares $\epsilon : V \to k$ e $\Delta : V \to V \otimes V$ satisfazendo counidade e coassociatividade; não é um objeto-comonoide porque o coproduto em $k\text{–}\mathsf{Vect}$ é $\oplus$, não $\otimes$).

Observação 4.5.12. Dada coálgebra C de dimensão finita, o dual de Cartier dá estrutura de álgebra (não necessariamente comutativa) em C^*. Se $I \subseteq C^*$ é ideal, sendo $D \coloneqq \bigcap_{f \in I} \operatorname{nuc} f$, então D é subcoálgebra. De fato, dado $c \in D$, escreva $\Delta c = \sum_i a_i \otimes b_i$ com número mínimo de parcelas (em particular $a_\bullet$ e $b_\bullet$ são linearmente independentes); então $(f \cdot g)c = \langle f, g\rangle(\Delta c) = \sum_i fa_i \cdot gb_i$; se $f \in I$ vale $f \cdot g \in I$, logo $0 = \sum_i fa_i \cdot gb_i$ para cada g, então $\sum_i fa_i \cdot b_i = 0$, e cada $fa_i = 0$ e $a_i \in D$; similarmente cada $b_i \in D$. Na outra direção, se $D \subseteq C$ é subcoálgebra, então $I \coloneqq \{f \in C^* \mid \forall_{d \in D} fd = 0\}$ é ideal. E, se $\dim C < \infty$, há bijeção entre os subespaços de C e os subespaços de C^*, o que dá bijeção entre subcoálgebras de C e ideais de C^*.

Teorema 4.5.13. *Se $A \subseteq B$ são k-álgebras de Hopf cocomutativas, então B é A-fielmente plana.*

Demonstração. Vale que B é união direcionada de B_i finitamente geradas, e cada $A \cap B_i$ é união direcionada de finitamente geradas $A_{i,j} \subseteq B_i$, e basta provar cada $A_{i,j} \to B_i$ fielmente plana (porque para provar $A \to B$ fielmente plana, sempre trabalhamos de cada vez só uma quantidade finita de elementos de A, B, e sempre algumas $A_{i,j} \subseteq B_i$ incluirão esses elementos). Então, SPDG, A, B são finitamente geradas. Também, SPDG, $k = \overline{k}$, por propriedades de tensores e extensão de escalares.

Mostra-se que toda subcoálgebra não nula minimal $C \subseteq B$ é com $\dim C = 1$: como C é união direcionada de coálgebras de dimensões finitas (similar à prova do lema 4.1.11), por minimalidade C é de dimensão finita; então C^* é k-álgebra (comutativa porque $C \subseteq B$ é cocomutativa) de dimensão finita; os ideais de C^* estão em bijeção com as subcoálgebras de C, então C^* só tem dois ideais, logo é corpo; então $C^* \subseteq \overline{k} = k$, e $1 = \dim C^* = \dim C$.

Cada subcoálgebra de dimensão um tem base c com $\Delta c = \lambda \cdot (c \otimes c)$ para algum $\lambda \in k$, logo $\Delta(\lambda \cdot c) = (\lambda \cdot c) \otimes (\lambda \cdot c)$; e $\langle \epsilon, 1 \rangle (\Delta c) = c = \lambda \cdot \epsilon c \cdot c$, logo $\epsilon(\lambda \cdot c) = 1$; então C é gerada por um elemento quase de grupo $\lambda \cdot c$.

Pelo lema 4.5.8(c), para mostrar B ser A-fielmente plana, basta B/A ser A-módulo plano.

Também B/A é um A–B-comódulo por: $\rho : B/A \to B \otimes B/A$ por $\rho[b] \coloneqq (1 \otimes \pi_{B/A})(\Delta b)$, definição válida porque se $b \in A$ então $\Delta b \in A \otimes A$, logo $(1 \otimes \pi_{B/A})(\Delta b) = 0$.

Temos que B/A é união direcionada de B-subcomódulos de k-dimensões finitas V. Logo, B/A é união direcionada dos $A \cdot V$, que são A–B-subcomódulos. Para mostrar que B/A é A-plano, basta que cada $A \cdot V$ seja A-plano. Mostraremos isso por indução em $\dim_k V$.

O caso $\dim_k V = 0$ é trivial. Supor $\dim_k V \geq 1$. Como $\rho(V) \subseteq B \otimes V$ tem dimensão finita, existe subcoálgebra não nula de dimensão finita $C \subseteq B$ com $\rho(V) \subseteq C \otimes V$. A k-álgebra (comutativa) C^* tem dimensão finita, logo nela cada ideal primo é maximal (como na prova do lema 3.1.16); então a interseção dos ideais maximais é o nilradical N.

Lembrar a ação $C^* \otimes V \xrightarrow{1 \otimes \rho} C^* \otimes C \otimes V \to V$. Há $m > 0$ com $N^m \cdot V = 0$ mas $N^{m-1} \cdot V \neq 0$. Seja $W \coloneqq N^{m-1} \cdot V$; logo $N \cdot W = 0$. Assim, W é um C^*/N-módulo; a álgebra C^*/N é reduzida, logo é produto de fatores $k = \overline{k}$; há $[e] \in C^*/N$ idempotente minimal com $e \cdot W \neq 0$ (porque a soma dos $[e]$ é 1 e $W \neq 0$), seja $\pi : C^*/N \to e \cdot C^*/N \cong k$ projeção; logo $e \cdot W$ é um C^*/M-módulo para $M \coloneqq \operatorname{nuc}(C^* \to C^*/N \xrightarrow{\pi} k)$ (codimensão 1); e como $e \cdot W$ é um C^*-submódulo, é um C-subcomódulo também. Então, se $f \in M$ e $w \in e \cdot W$ vale que $0 = f \cdot w = \langle f, 1 \rangle (\rho w)$, logo $\rho w \in \operatorname{nuc} f \otimes (e \cdot W)$; então, $\rho(e \cdot W) \subseteq (\bigcap_{f \in M} \operatorname{nuc} f) \otimes (e \cdot W)$. Seja $k \cdot a$ a

subcoálgebra minimal (onde a é quase de grupo) associada ao ideal maximal M, de modo que $\rho(e \cdot W) \subseteq (k \cdot a) \otimes e \cdot W$.

Definindo-se $\rho' : A \cdot V \to B \otimes A \cdot V$ por $A \cdot V \xrightarrow{\rho} B \otimes A \cdot V \xrightarrow{(a^{-1}\cdot)\otimes 1} B \otimes A \cdot V$, vale que ρ' é A–B-comódulo. Então: $\rho'(W' \coloneqq e \cdot W) \subseteq (a^{-1} \cdot R) \otimes W' = 1 \otimes W'$, e $\rho'(A \cdot W') \subseteq A \otimes A \cdot W'$.

Então temos $U \coloneqq A \cdot W'$, um A–A-subcomódulo de ρ'. Pelo lema 4.5.10, $A \cdot W'$ é então A-livre. O módulo $(A \cdot V)/(A \cdot W')$ (quociente de $A \cdot (V/W')$, $\dim(V/W') < \dim V$) é A–B-comódulo, e por hipótese indutiva é A-plano; então $A \cdot V$ é A-plano também. □

4.5.5 Os quocientes

Já sabemos que a categoria dos esquemas-afins afins abelianos algébricos tem limites finitos: incluindo o núcleo de $\eta : F \implies G$, que é $N \subseteq F$, onde $N(A) \coloneqq \{x \in F(A) \mid \eta_A(x) = 0\}$. Noutras palavras, o conúcleo do mapa de Hopf $f : A_G \to A_F$ é $A_F \to A_N = A_F/J$, onde J é o A_F-ideal gerado por $\{fa - \epsilon a \in A_F \mid a \in A_G\} = \{fa \in A_F \mid a \in \operatorname{nuc} \epsilon_{A_G}\}$. E os núcleos de mapas de Hopf:

Lema 4.5.14. *Dado $f : A \to B$ mapa de Hopf entre álgebras de Hopf cocomutativas, definindo-se $C \coloneqq \{a \in A \mid (f \otimes 1)(\Delta_A a) = 1_B \otimes a\}$, vale que $C \subseteq A$ é o equalizador de $f, \epsilon : A \to B$ na categoria das álgebras de Hopf cocomutativas.*

Demonstração. Vale que C é subálgebra (multiplicativa). Se $a \in C$, vale $Sa \in C$ porque $(f \otimes 1)(\Delta_A(Sa)) = (S \otimes S)((f \otimes 1)(\Delta_A a)) = 1_B \otimes Sa$ (cocomutatividade usada para $\Delta \circ S = (S \otimes S) \circ \Delta$; e f mapa de Hopf). Queremos mostrar $\Delta a \in C \otimes C$ para $a \in C$.

Se $a \in C$, sendo $\Delta_A a \coloneqq \sum_i b_i \otimes c_i$ com número mínimo de parcelas (em particular, (b_i) é linearmente independente, e (c_i) também), $(f \otimes 1)(\Delta_A a) = \sum_i fb_i \otimes c_i = 1_B \otimes a = \sum_i \epsilon b_i \otimes c_i$, e $fb_i = \epsilon b_i$; também

$$\begin{aligned}\textstyle\sum_i (f \otimes 1)(\Delta b_i) \otimes c_i &= (((f \otimes 1) \circ \Delta) \otimes 1) \textstyle\sum_i b_i \otimes c_i = ((f \otimes 1 \otimes 1) \circ (\Delta \otimes 1) \circ \Delta)a \\ &= ((f \otimes 1 \otimes 1) \circ (1 \otimes \Delta) \circ \Delta)a = \textstyle\sum_i fb_i \otimes \Delta c_i \\ &= \textstyle\sum_i \epsilon b_i \otimes \Delta c_i = 1 \otimes \Delta(\sum_i \epsilon b_i \cdot c_i) = 1 \otimes \Delta a = \sum_i 1 \otimes b_i \otimes c_i,\end{aligned}$$

logo $(f \otimes 1)(\Delta b_i) = 1 \otimes b_i$, logo $b_i \in C$; e também $c_i \in C$ por cocomutatividade. Portanto, $a \in C \implies \Delta a \in C \otimes C$; e assim C é subálgebra de Hopf.

Queremos provar que $C \to A$ é equalizador de $f, \epsilon : A \to B$. Primeiro, se $a \in C$, $\epsilon a = \langle 1, \epsilon \rangle (1_B \otimes a) = \langle 1, \epsilon \rangle ((f \otimes 1)(\Delta a)) = fa$. E se $g : D \to A$ é mapa de Hopf com $f \circ g = \epsilon_A \circ g = \epsilon_D$, vale para $d \in D$ que $gd \in C$ porque $(f \otimes 1)(\Delta(gd)) = (f \circ g \otimes g)(\Delta d) = (\epsilon_D \otimes g)(\Delta d) = 1 \otimes gd$. □

4.5.6 Subgrupos fechados de abelianos são núcleos

Queremos provar que cada $A \to A/J$, para A álgebra de Hopf cocomutativa e J é ideal de Hopf, é um conúcleo; equivale a ser conúcleo de seu núcleo $C \coloneqq \{a \in A \mid \Delta a - 1 \otimes a \in J \otimes A\}$, isto é, queremos que $J = A \cdot \operatorname{nuc} \epsilon_C$. Como C é preservado em extensão de escalares (isto é, $C \otimes \overline{k}$ é também o núcleo de $A \otimes \overline{k} \to (A \otimes \overline{k})/(J \otimes \overline{k})$, como se pode ver usando base de $\overline{k}$ sobre k), poderemos supor $k = \overline{k}$; e também poderemos supor A finitamente gerada. A ideia será usar comódulos com certos "vetores fixos" (com $\rho v \equiv 1 \otimes v \pmod{J \otimes V}$).

Definição 4.5.15. Dado comódulo $\rho : V \to A \otimes V$ e dado subespaço $W \subseteq V$, defina $I(W \subseteq V)$ como o menor ideal de Hopf I tal que $V \xrightarrow{\rho} A \otimes V \to A/I \otimes V$ leva W para dentro de $A/I \otimes W$.

Prova da existência: seja base $(v_i)_{i \in B}$ de W estendida a base $(v_i)_{i \in C}$ de V; escreva $\rho v_i = \sum_j a_{i,j} \otimes v_j$; a condição é que $\rho(W) \subseteq A \otimes W + I \otimes V$, isto é, que $a_{i,j} \in I$ para cada $i \in B$ e $j \notin B$; o ideal I gerado pelos $(a_{i,j}, Sa_{i,j})_{i \in B}^{j \notin B}$ é de fato ideal de Hopf: lembrar $\Delta a_{i,j} = \sum_l a_{i,l} \otimes a_{l,j}$, logo $i \in B$ e $j \notin B$ implica $\Delta a_{i,j} \in \sum_{l \in B} a_{i,l} \otimes a_{l,j} + \sum_{l \notin B} a_{i,l} \otimes a_{l,j} \in A \otimes I + I \otimes A$; etc.

Já vimos produto tensorial de dois comódulos. Também há potência exterior de comódulo $\rho : V \to A \otimes V$: $\rho' : \Lambda^M V \to A \otimes \Lambda^M V$, $\rho'(v_1 \wedge \cdots \wedge v_M) \coloneqq P(\rho v_1 \wedge \cdots \wedge \rho v_M)$ onde $P((a_1 \otimes w_1) \wedge \cdots \wedge (a_M \otimes w_M)) \coloneqq (a_1 \cdot \ldots \cdot a_M) \otimes (w_1 \wedge \cdots \wedge w_M)$. É quociente da estrutura de comódulo $V^{\otimes M}$. Lembrar que $\dim \Lambda^{\dim V} V = 1$.

Lema 4.5.16. *$I(W \subseteq V) = I(\Lambda^M W \subseteq \Lambda^M V)$ se $\dim W = M$ [não nulo] e $\dim V < \infty$.*

Demonstração. Seja $(v_i)_{i=1}^M$ base de W, estendida a base $(v_i)_{i=1}^N$ de V. Escreva $\rho v_i = \sum_j a_{i,j} \otimes v_j$. Então, $\Lambda^M V$ tem base $(v_{i_1} \wedge \cdots \wedge v_{i_M})_{i_1 < \cdots < i_M}$, e $\Lambda^M W = k \cdot (v_1 \wedge \cdots \wedge v_M)$. Logo,

$$\rho(v_1 \wedge \cdots \wedge v_M) = \sum_{j_1 < \cdots < j_M} \det(a_{\bullet, j_\bullet}) \otimes (v_{j_1} \wedge \cdots \wedge v_{j_M}).$$

Então $I(\Lambda^M W \subseteq \Lambda^M V)$ é o menor ideal de Hopf incluindo os $\det(a_{\bullet,j_\bullet})$ para sequências $(j_1 < \cdots < j_M)$ diferentes de $(1 < \cdots < M)$. E $I(W \subseteq V)$ é o menor ideal de Hopf incluindo $a_{i,j}$ para cada $1 \le i \le M$ e $M < j \le N$. Então, $I(\Lambda^M W \subseteq \Lambda^M V) \subseteq I(W \subseteq V)$. Agora lembramos $\sum_l a_{i,l} \cdot Sa_{l,j} = \langle 1, S \rangle(\Delta a_{i,j}) = \epsilon a_{i,j} = [i = j]$, logo $(a_{\bullet\bullet})$ é inversa da matriz $(Sa_{\bullet\bullet})$; há u inversível com $u \cdot Sa_{i,j} = (-1)^{i+j} \cdot \det(a_{J,I})_{J \neq j, I \neq i}$, que é determinante de matriz de ordem $N - 1$. Assim, para $1 \le i \le M$ e $M < j \le N$, pela expansão de Laplace generalizada,

$$\pm u \cdot Sa_{i,j} = \sum \pm \det(a_{J,I})_{1 \le J \le M}^{I \in (\cdots)} \cdot \det(a_{J,I})_{J > M,\ J \neq j}^{I \notin (\cdots)}$$

onde $(\cdots)$ varia pelos conjuntos de M índices em $\{1, \ldots, N\} \smallsetminus \{i\}$; como $1 \le i \le M$, $(\cdots)$ nunca será a sequência $(1 < \cdots < M)$, logo o primeiro fator estará em $I(\Lambda^M W \subseteq$

$\Lambda^M V$); então cada $Sa_{i,j}$, $1 \leq i \leq M$ e $M < j \leq N$, está em $I(\Lambda^M W \subseteq \Lambda^M V)$, e como este é ideal de Hopf, cada $a_{i,j}$ estará também, portanto $I(W \subseteq V) \subseteq I(\Lambda^M W \subseteq \Lambda^M V)$. □

Lema 4.5.17. *$I(W \otimes W' \subseteq V \otimes V') = I(W \subseteq V) + I(W' \subseteq V')$ se $W \subseteq V$ e $W' \subseteq V'$ [não nulos].*

Demonstração. Sendo como no lema anterior, W com base $(v_i)_{i \leq \dim W}$ estendida a base $(v_i)_{i \leq \dim V}$ de V, etc., escrevendo os comódulos $\rho v_i = \sum_j a_{i,j} \otimes v_j$ e $\rho' v'_i = \sum_j a'_{i,j} \otimes v'_j$, vale $\rho''(v_i \otimes v'_I) = \sum_{j,J} (a_{i,j} \cdot a'_{I,J}) \otimes (v_j \otimes v'_J)$. Logo $I(W \otimes W' \subseteq V \otimes V')$ é o menor ideal de Hopf incluindo os $a_{i,j} \cdot a'_{I,J}$ para: $1 \leq i \leq \dim W$, $1 \leq I \leq \dim W'$, $j > \dim W$ ou $J > \dim W'$; aí, $a_{i,j} \in I(W \subseteq V)$ ou $a'_{I,J} \in I(W' \subseteq V')$. Então temos $I(W \otimes W' \subseteq V \otimes V') \subseteq I(W \subseteq V) + I(W' \subseteq V')$. Para a outra direção, dado $a_{i,j} \in I(W \subseteq V)$ (com $i \leq \dim W < j$), então $a_{i,j} \cdot \det(a'_{\bullet\bullet}) = a_{i,j} \cdot u'$, inversível u', e expandindo o determinante, temos produtos $a_{i,j} \cdot a'_{1,J} \cdot \ldots$, que estarão em $I(W \otimes W' \subseteq V \otimes V')$, então $a_{i,j}$ também está; portanto $I(W \subseteq V) \subseteq I(W \otimes W' \subseteq V \otimes V')$ etc. □

Teorema 4.5.18. *Cada quociente de Hopf $A \to A/J$, onde A é cocomutativa, é um conúcleo.*

Demonstração. (De Takeuchi (1972) 4) Primeiro veja o final desta prova para saber o que se deseja fazer. SPDG, $k = \overline{k}$ e A é finitamente gerada (logo J também é ideal finitamente gerado). Escreva $J = \langle \xi_1, \ldots, \xi_\Xi \rangle$. Existe (assim como em 4.1.11) A-subcomódulo de dimensão finita $V \subseteq A$ (isto é, $\Delta V \subseteq A \otimes V$) incluindo $\xi_1, \ldots, \xi_\Xi$. Mostra-se $I(V \cap J \subseteq V) = J$: seja base $(v_i)_{i \leq \dim(V \cap J)}$, estendida a base (v_i) de V, escreva $\Delta v_i = \sum_j a_{i,j} \otimes v_j$; se $i \leq \dim(V \cap J)$, vale $\Delta v_i \in A \otimes J + J \otimes A$, logo cada $a_{i,j}$ (com $i \leq \dim(V \cap J) < j$) está em J; e $I(V \cap J \subseteq V) \subseteq J$; e também, $\langle 1, \epsilon \rangle(\Delta v_i) = v_i = \sum_j a_{i,j} \cdot \epsilon v_j = \sum_{j > \dim(V \cap J)} a_{i,j} \cdot \epsilon v_j$ porque $J \subseteq \operatorname{nuc} \epsilon$, logo cada v_i, $i \leq \dim(V \cap J)$, está em $I(V \cap J \subseteq V)$, e os elementos ξ_i também, portanto $J \subseteq I(V \cap J \subseteq V)$.

Temos então comódulo (de dimensão finita) $V \to A \otimes V$ com subespaço W com $I(W \subseteq V) = J$. Trocando-os por suas potências exteriores $\Lambda^{\dim W}$, como vimos acima obtemos $I(W \subseteq V) = J$ com adicionalmente $\dim W = 1$. A ação $W \to A/J \otimes W$ tem um único coeficiente b numa base $w \in W \smallsetminus 0$, e cada ação $W^{\otimes e} \to A/J \otimes W^{\otimes e}$ terá o coeficiente $[b^e]$ na base $w \otimes \cdots \otimes w$. Troque V e W por suas potências $(\_)^{\otimes e}$ onde e é escolhido como: se a característica é 0, $e = 1$ (e A é reduzida pelo teorema 4.5.2); se a característica é $p > 0$, então o nilradical de A é finitamente gerado (porque A é finitamente gerada), logo tem um índice de nilpotência n, e A^{p^n} é $k^{p^n} = k = \overline{k}$-subálgebra reduzida, logo escolha $e \coloneqq p^n$. Pelo lema anterior, continuamos com $I(W \subseteq V) = J + \cdots + J = J$, $\dim W = 1$.

Existe (w) base de W, escreva $\rho_{A/J} w \coloneqq [b^e] \otimes w$; logo b^e está numa subálgebra reduzida A^e; escrevendo $\rho v_i = \sum a_{i,j} \otimes v_j$ onde $v_0 = w$ e $a_{0,0} = b^e$, vale

$a_{0,1}, a_{0,2} \ldots \in J$, logo $\Delta b^e = \Delta a_{0,0} = \sum_j a_{0,j} \otimes a_{j,0} \in b^e \otimes b^e + J \otimes A$; e $\epsilon b^e = 1$. Em particular, $[b^e] \in A/J$ é quase de grupo. Procuremos um A-comódulo com elemento $w' \neq 0$ com $\langle \pi_{A/J}, 1\rangle(\rho' w') = [b^e]^{-1} \otimes w'$.

Seja U o subespaço gerado pelos $f \cdot b^e \coloneqq \langle f, 1\rangle(\Delta b^e)$, $f \in k\text{−}\mathsf{Alg}(A, k)$; é de dimensão finita pois está contido no subespaço gerado por segundos fatores de tensores em Δb^e. Mostra-se ser A-comódulo por meio de Δ. Seja $(u_\bullet)$ base de U, e seja $(u'_\bullet)$ base dum subespaço complementar em A; escreva $\Delta(f \cdot b^e) = \sum_i c_i \otimes u_i + \sum_j c'_j \otimes u'_j \in A^e \otimes A^e$; se por absurdo $\Delta(f \cdot b^e) \notin A \otimes U$, então existe $c'_j \neq 0$; e como $A^e \ni b^e$ é finitamente gerada reduzida sobre $k = \overline{k}$, o Nullstellensatz diz que existe $h' \in k\text{−}\mathsf{Alg}(A^e, k)$ (um "ponto") tal que $h'((c'_j)^e) \neq 0$; sendo $h : A \to k$ dada por $ha \coloneqq \sqrt[e]{h'(a^e)}$, temos $h \in k\text{−}\mathsf{Alg}(A, k)$ com $hc'_j \neq 0$; e assim $h \cdot (f \cdot b^e) = (h * f) \cdot (\Delta b^e) \in U$, onde $*$ é a operação de grupo em $k\text{−}\mathsf{Alg}(A, k)$, porém este elemento é $h \cdot (f \cdot b^e) = \sum_i hc_i \cdot u_i + \sum_j hc'_j \cdot u'_j$ onde $hc'_j \neq 0$, logo $h \cdot (f \cdot b^e) \notin U$, absurdo.

Para cada linear $g : A \to k$ com $g \restriction J = 0$, a cocomutatividade dá $g \cdot (f \cdot b^e) = f \cdot (g \cdot b^e) = f \cdot (gb^e \cdot b^e) = gb^e \cdot (f \cdot b^e)$ porque $\Delta b^e - b^e \otimes b^e \in J \otimes A$. Então, $\Delta(f \cdot b^e) \equiv b^e \otimes (f \cdot b^e) \pmod{J \otimes A}$ porque cada $\langle g, 1\rangle$ aplicado nos dois lados dá resultados iguais.

O A-comódulo U tem uma base u_i, com $\Delta u_i \coloneqq \sum_j c_{i,j} \otimes u_j$. Então, sendo U' espaço vetorial de base u'_i e definindo $\rho u'_i \coloneqq \sum_j Sc_{j,i} \otimes u'_j$, então é A-comódulo: $\langle \epsilon, 1\rangle(\rho u'_i) = \sum_j [j = i] \cdot u_j = u_i$; $(1 \otimes \rho)(\rho u'_i) = \sum_j Sc_{j,i} \otimes \rho u'_j = \sum_{j,l} Sc_{j,i} \otimes Sc_{l,j} \otimes u'_l = \sum_{j,l} (S \otimes S)(\tau(c_{l,j} \otimes c_{j,i})) \otimes u'_l = \sum_l \Delta(Sc_{l,i}) \otimes u'_l = (\Delta \otimes 1)(\rho u'_i)$. E como U satisfaz $[c_{i,j}] = [i = j] \cdot [b^e] \in A/J$, temos $[Sc_{j,i}] = [i = j] \cdot S[b^e] = [i = j] \cdot [b^e]^{-1}$.

O lema anterior dá $I(W \otimes k \cdot u'_1 \subseteq V \otimes U') = I(W \subseteq V) + I(k \cdot u'_1 \subseteq U') = J + I(k \cdot u'_1 \subseteq U') = J$, porque $I(k \cdot u'_1 \subseteq U')$ é o ideal gerado por $Sc_{j,1}, c_{j,1}$, para $j \neq 1$, que estão em J. E também, $w \otimes u'_1$, que gera $W \otimes k \cdot u'_1$, na estrutura de A/J-comódulo satisfaz $\rho_{A/J}(w \otimes u'_1) = ([b^e] \cdot [b^e]^{-1}) \otimes (w \otimes u'_1) = 1_{A/J} \otimes (w \otimes u'_1)$.

Portanto, temos A-comódulo de dimensão finita Z com elemento $z \neq 0$ tal que $I(k \cdot z \subseteq Z) = J$ e com $\rho z \equiv 1 \otimes z \pmod{J \otimes A}$. Seja base z_i de Z, onde $z_1 = z$, e escreva $\rho z_i \coloneqq \sum_j d_{i,j} \otimes z_j$; a hipótese em z dá $d_{1,i} \equiv [1 = i] \pmod J$. O ideal $I(k \cdot z \subseteq Z) = J$ é gerado por $d_{1,j}, Sd_{1,j}$ para $j \neq 1$. Temos $\Delta d_{1,j} = \sum_i d_{1,i} \otimes d_{i,j} = d_{1,1} \otimes d_{1,j} + \sum_{i \neq 1} d_{1,i} \otimes d_{i,j} \equiv 1 \otimes d_{1,j} \pmod{J \otimes A}$; então os geradores $d_{1,j}, Sd_{1,j}$ estão no conúcleo C de $A \to A/J$. Então, $J = A \cdot \operatorname{nuc} \epsilon_C$. □

4.5.7 A prova

Teorema 4.5.19. *A categoria dos esquemas-grupos afins abelianos (sobre corpo k) $\mathcal{C}$ é abeliana.*

Demonstração. A categoria já é pré-aditiva, tem o objeto inicial (e terminal), e todas as somas diretas. Vimos acima que existem todos os núcleos e os conúcleos. Resta tratar dos monomorfismos e os epimorfismos, nos dois lemas seguintes: ▽

Lema 4.5.20. *Em $\mathcal{C}$ todo monomorfismo é um núcleo.*

Demonstração. Seja $F : G \to H$ monomorfismo em $\mathcal{C}$, associado ao mapa de Hopf $f : A_H \to A_G$. Como $\operatorname{nuc} F \to G \xrightarrow{F} H$ é nulo e F é mônica, $\operatorname{nuc} F = 0$; isto é, F é componencialmente injetivo. Como para cada k-álgebra R, $F_R = (g \in k\text{−}\mathsf{Alg}(A_G, R)) \mapsto (g \circ f \in k\text{−}\mathsf{Alg}(A_H, R))$, vale que f é epimorfismo em $R\text{−}\mathsf{Alg}$.

Há decomposição $A_H \to f(A_H) \xrightarrow{\subseteq} A_G$ do epimorfismo f, logo $f(A_H) \subseteq A_G$ é continência epimórfica em $R\text{−}\mathsf{Alg}$. Pelo teorema 4.5.13, A_G é $f(A_H)$-fielmente plana, logo o corolário 4.5.7 implica $f(A_H) = A_G$. Então, sendo f sobrejetivo, $A_G \cong A_H/J$ para algum ideal J; portanto, pelo lema 4.5.18, $A_H \to A_G \cong A_H/J$ é um conúcleo. ▽

Lema 4.5.21. *Em $\mathcal{C}$ todo epimorfismo é um conúcleo.*

Demonstração. Seja $f : A_H \to A_G$ monomorfismo de álgebras de Hopf cocomutativas; seja $\pi : A_G \to A_G/\langle f(\operatorname{nuc} \epsilon_H)\rangle$ seu conúcleo; e seja $C \coloneqq \{a \in A_G \mid \Delta a - 1 \otimes a \in \langle f(\operatorname{nuc} \epsilon_H)\rangle \otimes A\}$ o núcleo do conúcleo. Pelo lema 2.9.4, conúcleo de núcleo de conúcleo é conúcleo, logo $C \to A_G$ tem o mesmo conúcleo $\pi : A_G \to A_G/\langle f(\operatorname{nuc} \epsilon_H)\rangle$.

Em termos de esquemas-grupos afins, há dois homomorfismos $F : G \to H$ e $F' : G \to G'$ (onde G' corresponde a C) com o mesmo núcleo; usando o produto-fibrado $G \times_H G = (R) \mapsto \{(g_0, g_1) \in GR \mid Fg_0 = Fg_1\}$, as duas setas $G \times_H G \rightrightarrows G \to G'$ coincidem; isto é, as duas setas $C \to A_G \rightrightarrows A_G \otimes_{A_H} A_G$ coincidem, isto é, $c \otimes 1 = 1 \otimes c \in A_G \otimes_{A_H} A_G$ para cada $c \in C$; como $f(A_H) \subseteq A_G$ é fielmente plana (pelo teorema 4.5.13) e pelo lema 4.5.6, temos que $C \subseteq f(A_H)$.

Fazendo o mesmo com $G \times_{G'} G \rightrightarrows G \to H$, concluímos $f(A_H) = C$. Portanto, $f : A_H \to A_G$ fatora-se como $A_H \to C \to A_G$, onde $C \to A_G$ é núcleo. Basta provar $A_H \to C$ isomorfismo.

Vale $A_H \to C$ é monomorfismo (porque $A_H \to A_G$ o é); e pelo lema anterior, como $A_H \to C$ é sobrejetivo, é um conúcleo. E por teoria de categorias, conúcleo mônico é isomorfismo. □

Corolário 4.5.22. *Se $A \subseteq B$ são k-álgebras de Hopf cocomutativas e B é finitamente gerada, então A também é.*

Demonstração. Seja $B \to B/J$, $J \coloneqq \langle \operatorname{nuc} \epsilon_A\rangle$ conúcleo de $A \to B$. Como B é finitamente gerada, J é ideal finitamente gerado; logo existe $A' \subseteq A$ subálgebra de Hopf finitamente gerada tal que $\langle \operatorname{nuc} \epsilon_{A'}\rangle$ inclui esses geradores de J e logo é J também; então $A' \to B$ tem o mesmo conúcleo que $A \to B$; como a categoria é abeliana, $A \to B$ e $A' \to B$ são monomorfismos logo núcleos de seu mesmo conúcleo; e núcleos são únicos a menos de isomorfismo, logo $A \cong A'$, finitamente gerada. □

Corolário 4.5.23. *As seguintes subcategorias da categoria dos esquemas-grupos afins abelianos (sobre corpo k) também são abelianas, com as mesmas somas, e os mesmos núcleos e conúcleos: (a) a dos algébricos; (b) a dos finitos.*

Demonstração. Os colimites finitos de álgebras de Hopf finitamente geradas (resp., de dimensões finitas) continuam o sendo; e o núcleo continua o sendo pelo corolário anterior. Então a mesma prova de que a categoria maior é abeliana pode ser copiada para as duas categorias menores. □

Observação 4.5.24. Epimorfismos de esquemas-grupos afins abelianos não precisam ser componencialmente sobrejetivos; por exemplo (se $k = \mathbb{F}_2$), $\underline{\alpha}_4 \to \underline{\alpha}_2$, $(R) \mapsto g \mapsto g^2$, é epimorfismo, pois $k[X]/(X^2) \to k[X]/(X^4)$, $X \mapsto X^2$, é injetivo, mas em $R \coloneqq k[X]/(X^2)$ o elemento $X \in \underline{\alpha}_2(R)$ não está na imagem de $\underline{\alpha}_4(R) = \{0, X\}$.

4.5.8 Multiplicatividade de ordens

Lema 4.5.25. *Se $0 \to G \to H \to K \to 0$ é sequência exata na categoria dos esquemas-grupos afins abelianos finitos, então $|H| = |G| \cdot |K|$ (onde $|\_|$ denota a ordem, isto é, dimensão da álgebra de Hopf).*

Demonstração. Ordens e sequências exatas são preservadas em extensão de escalares, logo supomos, SPDG, $k = \overline{k}$. Sejam $0 \leftarrow B \leftarrow A \leftarrow C \leftarrow 0$ as correspondentes álgebras de Hopf. Como $\overline{k}$ é perfeito, e temos cocomutatividade, temos decomposições $A \cong A_c \otimes A_r$ etc;. como a dimensão é finita, A_r é separável e A_c é local; a decomposição nos dois fatores é functorial, logo temos duas sequências exatas $0 \leftarrow B_x \leftarrow A_x \leftarrow C_x \leftarrow 0$ para $x \in \{c, r\}$, e basta considerar cada uma separadamente.

No caso $x = r$, pelo fato 4.2.4, temos estruturas de Hopf $A \cong k^{X_A}$, etc., para grupos abelianos finitos X_A, etc. Como $k^X \cong k[X]^*$ e o functor $k[\_]$ é pleno fiel, temos equivalentemente sequência exata $0 \to X_B \to X_A \to X_C \to 0$ de grupos abelianos finitos, logo $|X_C| = |X_A/X_B| = |X_A|/|X_B|$, e segue de $\dim_k A = |k^{X_A}|$ etc.

No caso $x = c$, cada ideal $\operatorname{nuc} \epsilon$ é nilpotente; pelo lema 4.5.3, A_c é C_c-livre, e como $A_c \otimes_{C_c} A_c \cong A_c \otimes_k B_c$ (porque $H \times_K H \cong H \times G$), vale $\dim_k A_c \cdot \dim_k B_c = \dim_k C_c \cdot \dim_{C_c}(A_c \otimes_{C_c} A_c) = \dim_k C_c \cdot (\dim_{C_C} A_c)^2$, e $\dim_k B_c = \dim_k C_c \cdot \dim A_c$, pois sempre álgebra de Hopf é não nula. □

Corolário 4.5.26. *Se $f : G \to H$ é morfismo entre esquemas-grupos afins abelianos finitos, vale que f é isomorfismo desde que: (a) f seja monomorfismo e $|G| \geq |H|$; ou (b) f seja epimorfismo e $|G| \leq |H|$.*

Prova de (a). Há sequência exata $0 \to G \xrightarrow{f} H \to C \to 0$, logo $|G| \cdot |C| = |H| \leq |G|$, logo $|C| = 1$ (pois $A_C \neq 0$, assim $|C| \neq 0$); assim $C = 0$, e f é isomorfismo. □

Capítulo 5

Mapas de Frobenius e Verschiebung

Lembremos que, quando k é corpo perfeito, toda álgebra de Hopf de dimensão finita cocomutativa é produto tensorial de quatro partes. Quando a característica é zero, pelo teorema 4.5.2 há só uma parte (reduzida de dual reduzida). Quando a característica é $p > 0$, veremos que as partes conexas serão onde certo mapa de Frobenius será "nilpotente", e as partes separáveis onde será "inversível"; e o mapa de Verschiebung classificará os duais.

5.1 Definição e propriedades básicas

Seja k corpo (depois suposto perfeito) de característica $p > 0$.

Definição 5.1.1. Define-se $\sigma : A \to A$ por $\sigma(a) = a^p$, que é aditivo (não necessariamente k-linear). Mas considere a extensão de escalares $A^{(p)} \coloneqq A \otimes_\sigma k =$ "$A \otimes \sigma^{-1}(k)$", com k-ação $\lambda\cdot(a\otimes\mu) = a\otimes\lambda\mu$, e os tensores satisfazendo $\mu^p(a\otimes\lambda) = a\otimes(\mu^p\lambda) = (\mu a)\otimes\lambda$. Então há o "mapa de Frobenius" $F : A^{(p)} \to A$, dado por $F(a \otimes \lambda) = \lambda a^p$, que é k-linear. (Como toda extensão de escalares, A álgebra de Hopf dá $A^{(p)}$ álgebra de Hopf; e assim F mapa de Hopf).

Observação 5.1.2. Se a álgebra A tem base $(a_i)_{i\in I}$ com $a_i \cdot a_j = \sum_l \alpha_{i,j,l} \cdot a_l$, então $A^{(p)}$ tem base $(a_i \otimes 1)_{i\in I}$ com $(a_i \otimes 1) \cdot (a_j \otimes 1) = \sum_l (\alpha_{i,j,l} \cdot a_l \otimes 1) = \sum_l a_l \otimes \alpha^p_{i,j,l}$; isto é, $A^{(p)}$ é quase a mesma álgebra que A, mas com as componentes da tabela de multiplicação elevadas a p; assim, se cada $\alpha_{i,j,l}$ está em $\mathbb{F}_p$, vale $A^{(p)} \cong A$.

Para estudarmos o dual do "Frobenius", precisamos da comultiplicação repetida, $\Delta^p : A \to A \otimes A \to \cdots \to A^{\otimes p}$.

Lema 5.1.3. *Seja V um k-espaço vetorial, denote por S o espaço dos tensores de $V^{\otimes p}$ invariantes em permutações. Então todo elemento de S é combinação linear de elementos da forma $v^{\otimes p} \coloneqq v \otimes \cdots \otimes v$, $v \in V$.*

Demonstração. Seja $(e_i)_{i\in I}$ base de V. O espaço S tem base de elementos da forma: dada função $f : I \to \mathbb{N}$ com $\sum_{i\in I} f(i) = p$, o elemento

$$e_f \coloneqq \sum_{(j_1,\dots,j_p)\in I^p} [f = (i \mapsto \operatorname{card}\{l \mid i = j_l\})] \cdot e_{j_1} \otimes \cdots \otimes e_{j_p}.$$

Basta mostrar que cada e_f é combinação linear dos $v^{\otimes p}$, $v \in V$. Os casos $e_f = e_i^{\otimes p}$ são triviais; logo, supomos $\forall_i f(i) < p$. Seja $I' \coloneqq \{i \mid f(i) \neq 0\}$, finito. Para $\alpha_{(\ )} : I' \to \mathbb{F}_p$, define-se $v_\alpha \coloneqq \sum_{i\in I'} \alpha_i \cdot e_i$. Então

$$\begin{aligned} v_\alpha^{\otimes p} &= \sum_{g:I'\to\mathbb{N}} [\sum_{i\in I'} g(i) = p] \cdot \big(\prod_{i\in I'} \alpha_i^{g(i)}\big) \cdot e_g \\ &= \sum_{g:I'\to\mathbb{N}_{<p}} [\sum_{i\in I'} g(i) = p] \cdot \big(\prod_{i\in I'} \alpha_i^{g(i)}\big) \cdot e_g + \sum_{i\in I'} \alpha_i^p \cdot e_i^{\otimes p}. \end{aligned}$$

Existe $i_0 \in I'$. Para $i \in I' \smallsetminus \{i_0\}$, denote M_i a matriz de Vandermonde para $0, \dots, p-1$, isto é, $M_i = (h^g)_{g,h\in\mathbb{N}_{<p}}$, inversível. Então $\bigotimes_{i\in I'\smallsetminus\{i_0\}} M_i$ é linear inversível também, representado pela matriz:

$$\left(\prod_{i\in I'\smallsetminus\{i_0\}} h(i)^{g(i)}\right)_{g,h:I'\smallsetminus\{i_0\}\to\mathbb{N}_{<p}}$$

Então, para cada $g' : I' \smallsetminus \{i_0\} \to \mathbb{N}_{<p}$, existem coeficientes $c_\bullet$ tais que:

$$E_{g'} = \sum_{h:I'\smallsetminus\{i_0\}\to\mathbb{N}_{<p}} c_h \cdot \sum_{g:I'\smallsetminus\{i_0\}\to\mathbb{N}_{<p}} \big(\prod_{i\in I'\smallsetminus\{i_0\}} h(i)^{g(i)}\big) \cdot E_g,$$

onde $E_\bullet$ denota os membros da base canônica de $k^{(I'\smallsetminus\{i_0\}\to\mathbb{N}_{<p})}$.

Temos mapa linear $E_g \mapsto e_{g\cup(i_0\mapsto p-S_g)}$ caso $S_g \coloneqq \sum_{i\in I'\smallsetminus\{i_0\}} g(i) \leq p$, e $E_g \mapsto 0$ caso contrário. Então,

$$\begin{aligned} e_f &= \sum_{h:I'\smallsetminus\{i_0\}\to\mathbb{N}_{<p}} c_h \cdot \sum_{g:I'\smallsetminus\{i_0\}\to\mathbb{N}_{<p}} \big(\prod_{i\in I'\smallsetminus\{i_0\}} h(i)^{g(i)}\big) \cdot [S_g \leq p] \cdot e_{g\cup(i_0\mapsto p-S_g)} \\ &= \sum_{\alpha:I'\to\mathbb{N}_{<p}}^{\alpha(i_0)=1} c_{\alpha\restriction(I'\smallsetminus\{i_0\})} \cdot \sum_{g:I'\to\mathbb{N}_{<p}} [\sum_{i\in I'} g(i) = p] \cdot \big(\prod_{i\in I'} \alpha_i{}^{g(i)}\big) \cdot e_g \\ &= \sum_{\alpha:I'\to\mathbb{N}_{<p}}^{\alpha(i_0)=1} c_{\alpha\restriction(I'\smallsetminus\{i_0\})} \cdot (v_\alpha^{\otimes p} - \sum_{i\in I'} \alpha_i^p \cdot e_i^{\otimes p}). \end{aligned}$$

□

Observação 5.1.4. Dada k-coálgebra cocomutativa A, dado $a \in A$, escrevendo $\Delta^p a$ (que é elemento simétrico de $A^{\otimes p}$ pela cocomutatividade) como $\sum_i \lambda_i \cdot v_i^{\otimes p}$, temos que para cada base

(e_j) de A, denotando por $[\cdots]$ os coeficientes na base induzida de $A^{\otimes p}$, vale: $[e_j^{\otimes p}](v_i^{\otimes p}) = ([e_j]v_i)^p$; então em $A^{(p)}$ vale $\sum_j e_j \otimes [e_j^{\otimes p}](\Delta^p a) = \sum_{j,i} e_j \otimes (\lambda_i \cdot ([e_j]v_i)^p) = \sum_{j,i} (e_j \cdot [e_j]v_i) \otimes \lambda_i = \sum_i v_i \otimes \lambda_i$. Em particular, como são sempre iguais, estes dois valores independem da base (e_j) e das parcelas $\lambda_i \cdot v_i^{\otimes p}$ específicas.

Definição 5.1.5. Dada k-coálgebra cocomutativa A, define-se $V : A \to A^{(p)}$ por: dada base (e_j), dado $a \in A$, define-se $Va \coloneqq \sum_j e_j \otimes [e_j^{\otimes p}](\Delta^p a)$; ou então escrevendo $\Delta^p a \coloneqq \sum_i \lambda_i \cdot v_i^{\otimes p}$, define-se $Va \coloneqq \sum_i v_i \otimes \lambda_i$. (Pela observação acima, esta definição é válida). Este V é o "mapa de Verschiebung", pronunciado "fèaxíbum"). V é k-linear.

Lema 5.1.6. *Se A é k-coálgebra cocomutativa de dimensão finita, então $V : A \to A^{(p)}$ é o dual de $F : A^{*(p)} \to A^*$ (módulo o isomorfismo canônico $A^{*(p)} \cong A^{(p)*}$).*

Demonstração. O dual de $V : A \to A^{(p)}$ é o mapa de $V^* : A^{(p)*} \to A^*$ dado por: $g \mapsto a \mapsto g(Va)$. Se $\iota : k \to K$ é extensão de corpos, o isomorfismo $(A^*)_K \cong (A_K)^*$ é dado por $f \otimes \lambda \mapsto a \otimes \mu \mapsto \iota(fa) \cdot \lambda \cdot \mu$. Aqui, ι é $\sigma : k \to k$, logo $\phi : A^{*(p)} \cong A^{(p)*}$ é dado por $f \otimes \lambda \mapsto a \otimes \mu \mapsto (fa)^p \cdot \lambda \cdot \mu$. Logo $A^{*(p)} \to A^{(p)*} \to A^*$ é dado por: sendo $\Delta^p a \coloneqq \sum_i \alpha_i \cdot a_i^{\otimes p}$, vale $Va = \sum_i a_i \otimes \alpha_i$, e $V^*(\phi(f \otimes \lambda))(a) = \phi(f \otimes \lambda)(Va) = \lambda \cdot \sum_i (fa_i)^p \cdot \alpha_i$. E o mapa $F : A^{*(p)} \to A^*$ é $f \otimes \lambda \mapsto (f^{\langle p \rangle} \circ \Delta^p) \cdot \lambda$, isto é, $F(f \otimes \lambda)(a) = f^{\langle p \rangle}(\Delta^p a) \cdot \lambda = \sum_i \alpha_i \cdot (fa_i)^p \cdot \lambda$. Então, F é $V^* \circ \phi$, como desejado. □

Lema 5.1.7. *Se A é k-álgebra de Hopf cocomutativa, então $V : A \to A^{(p)}$ é mapa de Hopf.*

Demonstração. Como $\Delta^p 1 = 1 \cdot 1^{\otimes p}$, vale $V1 = 1 \otimes 1$. Dados $a, b \in A$ com $\Delta^p a \coloneqq \sum_i \alpha_i \cdot a_i^{\otimes p}$ e $\Delta^p b \coloneqq \sum_j \beta_j \cdot b_j^{\otimes p}$, vale $\Delta^p(a \cdot b) = \sum_{i,j} \alpha_i \cdot \beta_j \cdot (a_i \cdot b_j)^{\otimes p}$, então $V(a \cdot b) = \sum_{i,j} a_i \cdot b_j \otimes \alpha_i \cdot \beta_j = Va \cdot Vb$. E A é união direcionada de coálgebras de dimensões finitas C_j, e $V : A \to A^{(p)}$ restringe-se a $V : C_j \to C_j^{(p)}$; como $V \restriction C_j$ é dual de $F : C_j^{*(p)} \to C_j^*$, que preserva a multiplicação, $V \restriction C_j$ preserva a comultiplicação Δ; então $V : A \to A^{(p)}$ preserva Δ também. □

Lema 5.1.8. *Se A é k-álgebra de Hopf cocomutativa, então $F \circ V : A \to A$ é o mapa $(\cdot^p) \circ \Delta^p$ (onde $(\cdot^p) : A^{\otimes p} \to A$, $(\cdot^p)(a_1 \otimes \cdots \otimes a_p) \coloneqq a_1 \cdots a_p$), e $V \circ F : A^{(p)} \to A^{(p)}$ é o mapa $(\cdot^p) \circ \Delta^p$.*

Demonstração. Escreva $\Delta^p a \coloneqq \sum_i \alpha_i \cdot a_i^{\otimes p} = \sum_i (\alpha_i \cdot a_i) \otimes a_i^{\otimes (p-1)}$; logo $Va = \sum_i a_i \otimes \alpha_i$. Então, $F(Va) = \sum_i \alpha_i \cdot a_i^p = (\cdot^p)(\Delta^p a)$. Também, $F(a \otimes 1) = a^p$, $\Delta^p a^p = \sum_i \alpha_i^p \cdot (a_i^p)^{\otimes p}$, $Va^p = \sum_i a_i^p \otimes \alpha_i^p$, logo $V(F(a \otimes 1)) = Va^p = \sum_i a_i^p \otimes \alpha_i^p$, e $(\cdot^p)(\Delta^p(a \otimes 1)) = (\cdot^p)(\sum_i (\alpha_i \cdot a_i \otimes 1) \otimes (a_i \otimes 1)^{\otimes (p-1)}) = (\cdot^p)(\sum_i \alpha_i^p \cdot (a_i \otimes 1)^{\otimes p}) = \sum_i a_i^p \otimes \alpha_i^p$. □

Então, se G é esquema-grupo afim abeliano, há homomorfismos $F : G \to G^{(p)}$ e $V : G^{(p)} \to G$ com $F \circ V$ e $V \circ F$ sendo os respectivos $g \mapsto p \cdot g$.

5.1.1 Relacionando-os com álgebras separáveis, conexas

Lema 5.1.9. *Dada uma k-álgebra de Hopf A cocomutativa de dimensão finita:*

1. *A é conexa sse existe N tal que*

$$\left(A \leftarrow k \overset{\epsilon_{A^{(p)^N}}}{\leftarrow} A^{(p)^N}\right) = \left(A \overset{F_A}{\leftarrow} A^{(p)} \overset{F_{A^{(p)}}}{\leftarrow} A^{(p)(p)} \leftarrow \cdots \leftarrow A^{(p)^N}\right).$$

2. *A é separável sse $F : A^{(p)} \to A$ é isomorfismo;*

Demonstração. (1) Lembrar que A é conexa (isto é, local, pois dimensão finita) sse seu ideal maximal $\operatorname{nuc}\epsilon$ é nilpotente; isso sse algum mapa $F_A \circ \cdots \circ F_{A^{(p)^{N-1}}}$ se anula em $\operatorname{nuc}\epsilon$, pois as imagens desse mapa são as somas de elementos $(\cdots(a^p \cdot \lambda_0)\cdots\lambda_{N-1})^p$, $a \in \operatorname{nuc}\epsilon_A$.

(2) Sendo $A = \prod_i A_i$, A_i locais, vale $F_A = \prod_i F_{A_i}$, logo consideramos cada fator A_i por vez. Quando A_i não é reduzida, F não é injetivo. Supor A_i reduzida (isto é, corpo). Caso A_i seja separável: mostremos F_{A_i} sobrejetivo (em particular bijetivo); seja $a \in A_i \smallsetminus F_{A_i}(A_i^{(p)})$; vale que $k[a^p] \subseteq k[a] \subseteq A_i$ são corpos (de dimensões finitas), a satisfaz $X^p - a^p$, que se fatora $(X-a)^p$, logo é irredutível em $k[a^p] \not\ni a$, logo é seu polinômio mínimo, porém é inseparável; assim $k[a^p] \subseteq k[a]$ é inseparável, e a extensão maior $k \subseteq A_i$ também, contradição.

E caso F_{A_i} seja bijetivo, dado $a \in A_i$, vale que $F : k[a]^{(p)} \to k[a]$ é injetivo também, logo sobrejetivo, logo há $P(X) \in k[X]$ com $a = P(a^p)$, isto é, a satisfaz $X - P(X^p)$, que é polinômio separável porque sua derivada é $1 - 0 \perp X - P(X^p)$; então A_i é separável. □

Definição 5.1.10. Abrevia-se

$$(F_A^N : A^{(p)^N} \to A) \coloneqq F_A \circ F_{A^{(p)}} \circ \cdots \circ F_{A^{(p)^{N-1}}},$$
$$(V_A^N : A \to A^{(p)^N}) \coloneqq V_{A^{(p)^{N-1}}} \circ \cdots \circ V_{A^{(p)}} \circ V_A.$$

Definição 5.1.11. Diz-se que G é de tipo x-y quando G é x e seu dual G^* é y. (Assim, por exemplo, um esquema-grupo afim abeliano finito G é de tipo local-local se e só se F e V são "nilpotentes").

Capítulo 6

Vetores de Witt

Queremos classificar esquemas-grupos afins abelianos finitos por meio de seus homomorfismos a um objeto específico, que será um esquema-anel afim de dimensão infinita a ser procurado. Seus elementos serão vetores $(r_0, r_1, \ldots)$ com operações especiais. Sua álgebra de Hopf é então $k[X_0, X_1, \ldots]$ com certo Δ, o mapa F é $X_i \mapsto X_i^p$, logo $F(r_0, r_1, \ldots) \coloneqq (r_0^p, r_1^p, \ldots)$. Tentaremos que Verschiebung seja $V(r_0, r_1, \ldots) \coloneqq (0, r_0, r_1, \ldots)$; logo, $p \cdot (r_0, r_1, \ldots) = V(F(r_0, r_1, \ldots)) = (0, r_0^p, r_1^p, \ldots)$. As operações $+$ e $\cdot$ deverão ter certa sofisticação.

Tentaremos fazer que a n-ésima componente do resultado (de cada soma ou produto) só dependa das componentes i-ésimas, $0 \leq i \leq n$, dos argumentos; em particular, serão operações "contínuas". Tentaremos também que valha $(r_0, r_1, \ldots) = \sum_{i=0}^{\infty}(0^{(i)}, r_i, 0^{(\infty)}) = \sum_{i=0}^{\infty} p^i \cdot \tau(r_i^{1/p_i})$ onde $\tau(x) \coloneqq (x, 0, 0, \ldots)$, e onde consideramos elementos $r_0, r_1, \ldots$ num corpo perfeito. Resta calcular $\tau(x) + \tau(y)$.

Queremos que hajam $\Phi_n(r_0, \ldots) \in k$ (dependendo só das n primeiras componentes) que preservem $+$ e $\cdot$. Em particular, deve valer $\Phi_n(r_0, \ldots) = \sum_{i=0}^{n} \Phi_n(0^{(i)}, r_i, 0^{(\infty)}) =: \sum_{i=0}^{n} \Phi_{n,i}(r_i)$; e também, $p \cdot \Phi_n(0^{(i)}, r_i, 0^{(\infty)}) = \Phi_n(p \cdot (0^{(i)}, r_i, 0^{(n-1-i)})) = \Phi_n(0^{(i+1)}, r_i^p, \cdots)$, isto é, $p \cdot \Phi_{n,i}(r_i) = \Phi_{n,i+1}(r_i^p)$. Então tentaremos polinômios $\Phi_{n,0}(x)$, $\ldots, \Phi_{n,n}(x)$ sendo respectivamente: $x^{p^n}, p \cdot x^{p^{n-1}}, \ldots, p^n \cdot x$.

6.1 A definição dos vetores de Witt

Lema 6.1.1. *Se I é ideal de anel R e $p \in \mathbb{N}$ é primo com $p \in I$, então $\forall_{n \in \mathbb{N}} a \equiv b \pmod{I} \implies a^{p^n} \equiv b^{p^n} \pmod{I^{n+1}}$.*

Demonstração. Por indução em n, basta provar $a \equiv b \pmod{I^m} \implies a^p \equiv b^p \pmod{I^{m+1}}$. De fato, sendo $c \coloneqq a - b \in I^m$, vale (usando que $\binom{p}{1}, \ldots, \binom{p}{p-1}$ são múltiplos do primo p) $a^p - b^p = (c + b)^p - b^p = c^p + \sum_{i=1}^{p-1} \binom{p}{i} \cdot c^i \cdot b^{p-i} \in (I^{pm} \subseteq I^{m+1}) + \sum_{i=1}^{p-1} p \cdot (I^{im} \subseteq I^m) \subseteq I^{m+1}$. □

Definição 6.1.2. Define-se esquema afim W sobre $\mathbb{Z}$ como $W(R) \coloneqq R \times R \times \cdots$ para cada anel R (isto é, $\mathbb{Z}$-álgebra R).

Definição 6.1.3. Temos a operação de "componente-fantasma": $\Phi_n : W(R) \to R$, $\Phi_n(\vec{x}) \coloneqq \sum_{i=0}^{n} p^i \cdot x_i^{p^{n-i}}$.

O objetivo será mostrar que há única estrutura de esquema-anel em W, de modo que cada Φ_n seja homomorfismo.

Lema 6.1.4. *Sendo $I : \mathbb{Z}-\mathsf{Alg} \to \mathsf{Conj}$ o functor $I(R) \coloneqq R$, dado mapa natural $u : I \times I \implies I$, satisfazendo, para cada anel R e cada $n \in \mathbb{N}$,*

$$\forall_{a,b,x,y \in R} u_R(a + p^n x, b + p^n y) - u_R(a, b) \in p^n \cdot \mathbb{Z}[a, b, x, y],$$

então existe único mapa natural $v : W \times W \implies W$ tal que

$$\forall_{n \geq 0} \forall_{\vec{x},\vec{y}} \Phi_n(v(\vec{x}, \vec{y})) = u\left(\Phi_n(\vec{x}), \Phi_n(\vec{y})\right).$$

Demonstração. Basta trabalhar no anel de polinômios $R = \mathbb{Z}[x_0, y_0, x_1, y_1, \ldots]$. Desejamos resolver: $\Phi_n \vec{z} = u(\Phi_n \vec{x}, \Phi_n \vec{y})$, isto é,

$$n = 0 \implies z_0 = u\left(x_0, y_0\right),$$

$$n \geq 1 \implies p^n \cdot z_n + \Phi_{n-1}(\vec{z}^{\sigma}) = u\left(\Phi_n \vec{x}, \Phi_n \vec{y}\right),$$

onde $\vec{z}^{\sigma}$ denota $(z_0^p, z_1^p, \ldots)$. Como $\Phi_{n-1}(\vec{z}^{\sigma})$ só depende das $z_0, \ldots, z_{n-1}$, até agora sabe-se que há única solução

$$z_n \coloneqq v_n(\vec{x}, \vec{y}) \in \mathbb{Z}[1/p][x_0, y_0, \ldots, x_n, y_n],$$

e resta mostrar, por indução em n, que os coeficientes de z_n são na verdade inteiros.

Caso $n = 0$, trivial, pois $z_0 = u(x_0, y_0) \in \mathbb{Z}[x_0, y_0]$, já que todo mapa natural $u : I \times I \implies I$ é necessariamente dado por um polinômio fixo nos dois argumentos.

Supor $n \geq 1$. Temos

$$\begin{aligned} z_n &= \frac{u(\Phi_n\vec{x}, \Phi_n\vec{y}) - \Phi_{n-1}(\vec{z}^{\sigma})}{p^n} \\ &= \frac{u(\Phi_{n-1}(\vec{x}^{\sigma}) + p^n x_n, \Phi_{n-1}(\vec{y}^{\sigma}) + p^n y_n) - \Phi_{n-1}(\vec{z}^{\sigma})}{p^n} \\ &\in \frac{u(\Phi_{n-1}(\vec{x}^{\sigma}), \Phi_{n-1}(\vec{y}^{\sigma})) - \Phi_{n-1}(\vec{z}^{\sigma}) + p^n \cdot R}{p^n} \\ &= \frac{\Phi_{n-1}(v(\vec{x}^{\sigma}, \vec{y}^{\sigma})) - \Phi_{n-1}(\vec{z}^{\sigma})}{p^n} + R \\ &= \sum_{i=0}^{n-1} \frac{p^i}{p^n} \cdot \left(v_i(\vec{x}^{\sigma}, \vec{y}^{\sigma})^{p^{n-1-i}} - (z_i^p)^{p^{n-1-i}} \right) + R. \end{aligned}$$

Cada parcela está em R, porque

$$v_i(\vec{x}^{\sigma}, \vec{y}^{\sigma})^{p^{n-1-i}} - v_i(\vec{x}, \vec{y})^{p \cdot p^{n-1-i}} \in (p \cdot R)^{p^{n-i}} = \frac{p^n}{p^i} \cdot R,$$

por aplicação do lema 6.1.1 a $v_i(\vec{x}^{\sigma}, \vec{y}^{\sigma}) - v_i(\vec{x}, \vec{y})^p \in p \cdot R,\ i \leq n-1$, hipótese indutiva. □

Teorema 6.1.5. *Há única estrutura de esquema-anel em W (chamado esquema-anel dos vetores de Witt p-ádicos) de modo que as componentes-fantasmas $\Phi_n : W(R) \to R$ sejam homomorfismos naturais.*

Demonstração. Aplicamos o lema anterior ao mapa $u : I \times I \implies I,\ u(x, y) \coloneqq x - y$, com

$$u_R(a + p^n x, b + p^n y) - u_R(a, b) = p^n x + p^n y \in p \cdot \mathbb{Z}[a, b, x, y],$$

e depois ao mapa $u(x, y) \coloneqq xy$, com

$$u_R(a + p^n x, b + p^n y) - u_R(a, b) = p^n \left(xb + ay + p^n xy \right) \in p^n \cdot \mathbb{Z}[a, b, x, y],$$

e depois usamos as unicidades para mostrar os mapas obtidos $W \times W \implies W$ dão uma estrutura de esquema-anel. □

Exemplo 6.1.6. Em $(x_0, x_1, \ldots) \pm (y_0, y_1, \ldots) = (z_0, z_1, \ldots)$, temos:

$$z_0 = x_0 \pm x_1,$$

$$\begin{aligned} z_1 &= \frac{\Phi_1\vec{x} \pm \Phi_1\vec{y} - \Phi_0(\vec{z}^{\sigma})}{p} \\ &= \frac{x_0^p + px_1 \pm (y_0^p + py_1) - z_0^p}{p} \\ &= x_1 \pm y_1 + \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} \cdot x_1^i \cdot (\pm y_1)^{p-i}, \cdots \end{aligned}$$

Fato 6.1.7. *(a) O mapa $\tau : R \to W(R)$ dado por $x \mapsto (x, 0, 0, \ldots)$ é multiplicativo.*

(b) Dado $X \subseteq \mathbb{N}$, dado $\vec{x} \in W(R)$, vale

$$\vec{x} = \left(\begin{cases} x_i & (i \in X) \\ 0 & (i \notin X) \end{cases} \right)_{i \in \mathbb{N}} + \left(\begin{cases} 0 & (i \in X) \\ x_i & (i \notin X) \end{cases} \right)_{i \in \mathbb{N}}.$$

(c) Vale $(a, 0, 0, \ldots) \cdot (x_0, x_1, \ldots) = (a^{p^0} \cdot x_0, a^{p^1} \cdot x_1, \ldots)$.

Demonstração. (a) Vale $\tau(1) = (1, 0, \ldots)$, e $\Phi_n(\tau(1)) = 1^{p^n} = 1$, elemento neutro. Também,

$$\Phi_n(\tau(x) \cdot \tau(y)) = \Phi_n(\tau(x)) \cdot \Phi_n(\tau(y)) = x^{p^n} \cdot y^{p^n} = (xy)^{p^n} = \Phi_n(\tau(xy)),$$

para cada anel R e quaisquer $x, y \in R$, logo $\tau(x) \cdot \tau(y) = \tau(xy)$.

(b) Sendo y e z as duas parcelas do enunciado,

$$\Phi_n(y + z) = \sum_{0 \leq i \leq n}^{i \in X} p^i \cdot x_i^{p^{n-i}} + \sum_{0 \leq i \leq n}^{i \notin X} p^i \cdot x_i^{p^{n-i}} = \Phi_n(x).$$

(c) Vale

$$\begin{aligned} \Phi_n\left(a^{p^0}x_0, a^{p^1}x_1, \ldots\right) &= \sum_{0 \leq i \leq n} p^i \cdot a^{p^i \cdot p^{n-i}} \cdot x_i^{p^{n-i}} \\ &= a^{p^n} \cdot \sum_{0 \leq i \leq n} p^i \cdot x_i^{p^{n-i}} = \Phi_n(a, 0, \ldots) \cdot \Phi_n(x_0, x_1, \ldots). \end{aligned}$$

□

Observação 6.1.8. Para cada $n \in \mathbb{N}$, define-se $W_n(R) \coloneqq W(R)/I_n$, onde $I_n \coloneqq \{x \in W(R) \mid 0 = x_0 = \cdots = x_{n-1}\}$; então W_n é esquema-anel, cujos elementos são os "vetores de Witt" p-ádicos de comprimento n.

6.1.1 Relação com os p-ádicos

Fato 6.1.9. *Sendo $\mathbb{Z}_p$ o anel dos inteiros p-ádicos, vale $\mathbb{Z}_p \cong W(\mathbb{F}_p)$.*

Demonstração. Temos o diagrama comutativo:

$$\begin{array}{ccccccc} \mathbb{Z}/p^0 & \longleftarrow & \mathbb{Z}/p^1 & \longleftarrow & \mathbb{Z}/p^2 & \longleftarrow & \cdots \\ \downarrow & & \downarrow & & \downarrow & & \\ W_0(\mathbb{F}_p) & \longleftarrow & W_1(\mathbb{F}_p) & \longleftarrow & W_2(\mathbb{F}_p) & \longleftarrow & \cdots \end{array}$$

Cada coluna é o mapa $\mathbb{Z}/p^n \to W_n(\mathbb{F}_p)$ dado por $[m] \mapsto m \cdot (1, 0^{n-1})$; é injetivo porque $p^{n-1} \cdot (1, 0^{n-1}) = (0^{n-1}, 1) \neq 0$; e é bijetivo porque o domínio e o contradomínio têm a mesma cardinalidade, p^n. Logo os mapas verticais formam um isomorfismo natural entre as duas linhas; tomando limites, temos $\mathbb{Z}_p \cong W(\mathbb{F}_p)$. □

6.1.2 Usando séries geradoras

Sendo R uma $\mathbb{Z}[1/p]$-álgebra, dado $\vec{x} \in W(R)$, podemos considerar a série geradora

$$\begin{aligned} L(\vec{x}, t) &\coloneqq \sum_{n\geq 0} \Phi_n(\vec{x}) \cdot \frac{t^{p^n}}{p^n} = \sum_{n\geq 0} \sum_{i=0}^{n} p^i \cdot x_i^{p^{n-i}} \cdot \frac{t^{p^n}}{p^n} \\ &= \sum_{i\geq 0} \sum_{d\geq 0} p^i \cdot x_i^{p^d} \cdot \frac{t^{p^{i+d}}}{p^{i+d}} = \sum_{i\geq 0} \sum_{d\geq 0} \frac{(x_i \cdot t^{p^i})^{p^d}}{p^d} = \sum_{i\geq 0} S(x_i \cdot t^{p^i}) \end{aligned}$$

onde $S(t) \coloneqq \sum_{d\geq 0} t^{p^d}/p^d$. (Já se entenderá por que $\Phi_n(\vec{x})/p^n$ em vez de $\Phi_n(\vec{x})$.)

Notar que $\log \frac{1}{1-t^n} = t^n + t^{2n}/2 + t^{3n}/3 + \cdots$. Encontraremos c_n com

$$S(t) = \sum_{n\geq 1} c_n \cdot \log \frac{1}{1-t^n} = \sum_{n\geq 1} \sum_{m\geq 1} c_n \cdot \frac{t^{mn}}{m} = \sum_{a\geq 1} t^a \cdot \sum_{m \sqsubseteq a} \frac{c_{a/m}}{m},$$

onde $\sqsubseteq$ denota a relação de divisibilidade. Devemos ter

$$a = p^d \implies \sum_{m\sqsubseteq a} \frac{c_{a/m}}{m} = \frac{1}{p^d}, \quad a \notin \{p^0, p^1, \ldots\} \implies \sum_{m\sqsubseteq a} \frac{c_{a/m}}{m} = 0.$$

Usando a linguagem de funções aritméticas multiplicativas (e $*$ sendo convolução), temos $c_{(\ )} * e_{-1} = f$, onde $e_{-1}(m) = 1/m$ e $f(p^d) = 1/p^d$ e $f(a) = 0$ se $a \notin \{p^0, p^1, \ldots\}$. Assim, pela fórmula de inversão de Möbius,

$$c_{(\ )} * e_{-1} * (\mu \cdot e_{-1}) = c_{(\ )} = f * (\mu \cdot e_{-1}),$$

$$c_a = \sum_{p^e \sqsubseteq a} \frac{1}{p^e} \cdot \mu\left(\frac{a}{p^e}\right) \cdot \frac{p^e}{a} = \frac{1}{a} \cdot \sum_{p^e \sqsubseteq a} \mu\left(\frac{a}{p^e}\right).$$

Para $a = p^d$, temos $c_a = a^{-1} \cdot \sum_{e \le d} \mu(p^{d-e}) = a^{-1} \cdot [a = 1]$; e se a não é potência de p, vale $a = p^d \cdot m$ com $p \not\mid m \ge 2$, e

$$\begin{aligned} c_a &= a^{-1} \cdot \sum_{e \le d} \mu\left(p^{d-e} \cdot m\right) = a^{-1} \cdot \begin{cases} \mu(m) & (d = 0) \\ \mu(m) - \mu(m) + 0 \cdots & (d \ge 1) \end{cases} \\ &= \frac{\mu(a)}{a} \cdot [d = 0]. \end{aligned}$$

Conclui-se:

Fato 6.1.10. *Vale:*

$$S(t) = \sum_{d \ge 0} \frac{t^{p^d}}{p^d} = \sum_{n \not\mid p} \frac{\mu(n)}{n} \cdot \log \frac{1}{1 - t^n}.$$

Assim,

$$\begin{aligned} \exp\left(-L(\vec{x}, t)\right) &= \exp\left(-\sum_{n \ge 0} \frac{\Phi_n(\vec{x})}{p^n} \cdot t^{p^n}\right) \\ &= \prod_{i \ge 0} \exp\left(-S(x_i \cdot t^{p^i})\right) \\ &= \prod_{i \ge 0} \exp\left(\sum_{n \not\mid p} \frac{\mu(n)}{n} \cdot \log\left(1 - x_i^n \cdot t^{n \cdot p^i}\right)\right) \\ &= \prod_{i \ge 0} \prod_{n \not\mid p} \left(1 - x_i^n \cdot t^{n \cdot p^i}\right)^{\mu(n)/n}. \end{aligned}$$

Então $E(\vec{x}, t) \coloneqq \exp(-L(\vec{x}, t))$ é uma série em t cujos coeficientes são polinômios em $\mathbb{Z}_{(p)}[x_0, x_1, \ldots]$, onde $\mathbb{Z}_{(p)}$ é o anel dos racionais cujos denominadores são coprimos a p.

Demonstração. Para $n \not\mid p$, $(1 - y)^{\mu(n)/n} = \sum_{m \ge 0} \binom{\mu(n)/n}{m} \cdot (-y)^m$ onde também para $x \notin \mathbb{Z}$ se define $\binom{x}{m}$, que para $x = \mu(n)/n$ é um racional de denominador dividindo n^m, coprimo a p. □

6.1.3 Frobenius e Verschiebung nos vetores de Witt

O esquema afim W pode ser restringido a $\mathbb{F}_p$-álgebras (também denotado W); assim $W^{(p)} \cong W$ (pois, lembrando, $\lambda^p = \lambda$ para $\lambda \in \mathbb{F}_p$). Podemos logo considerar os mapas de Frobenius e Verschiebung como $F, V : W \to W$. Vale $F(x_0, x_1, \ldots) = (x_0^p, x_1^p, \ldots)$, para quaisquer $(x_0, x_1, \ldots) \in W(R)$ e $\mathbb{F}_p$-álgebra R. Assim F é mapa aditivo e multiplicativo (porque os coeficientes de $x \pm y$ e $x \cdot y$ são polinômios $P(x_0, y_0, \ldots) \in \mathbb{F}_p[x_0, y_0, \ldots]$, e temos que $P(x_0, y_0, \ldots)^p = P(x_0^p, y_0^p, \ldots)$).

Para obter a fórmula de V, primeiro $V(F\vec{x}) = p \cdot \vec{x}$. Usamos a série geradora

da seção anterior. Primeiro para $\vec{x} \in W(R)$ onde $R = \mathbb{Q}[x_0, x_1, \ldots]$ (não uma $\mathbb{F}_p$-álgebra), vale

$$E(p \cdot \vec{x}, t) = \exp(-L(p \cdot \vec{x}, t)) = \exp\left(-\sum_{n \geq 0} \frac{p \cdot \Phi_n(\vec{x})}{p^n} \cdot t^{p^n} \right) = \exp\left(-L(\vec{x}, t)\right)^p ;$$

então $E(p \cdot \vec{x}, t) = E(\vec{x}, t)^p$ para qualquer álgebra contendo os coeficientes de E, isto é, para qualquer $\mathbb{Z}_{(p)}$-álgebra R e $\vec{x} \in W(R)$. Em particular vale para qualquer $\mathbb{F}_p$-álgebra R, pois todo inteiro coprimo a p é inversível em $\mathbb{F}_p$. Neste caso $E(\vec{x}, t)^p$ é a série obtida elevando cada termo a p, e cada coeficiente é um polinômio em $\mathbb{F}_p[x_0, x_1, \ldots]$, logo temos

$$\begin{aligned} E(\vec{x}, t)^p &= \prod_{i \geq 0} \prod_{n \not\equiv p} \left(1 - x_i^n \cdot t^{n \cdot p^i}\right)^{p \cdot \mu(n)/n} \\ &= \prod_{i \geq 0} \prod_{n \not\equiv p} \left(1 - x_i^{n \cdot p} \cdot t^{n \cdot p^{i+1}}\right)^{\mu(n)/n} = E((0, x_0^p, x_1^p, \ldots), t). \end{aligned}$$

Portanto, $p \cdot (x_0, x_1, \ldots) = (0, x_0^p, x_1^p, \ldots) \quad (\vec{x} \in W(R),\ R \in \mathbb{F}_p\text{–}\mathsf{Alg})$.

O mapa $F : W \to W$ é epimorfismo, pois a nível de álgebra de Hopf $A_W = k[X_0, X_1, \ldots]$ é o mapa $X_i \mapsto X_i^p$, que é injetivo (logo monomorfismo). Assim a igualdade $V(F\vec{x}) = p \cdot \vec{x}$ caracteriza unicamente o mapa V: $V(\vec{x}) = (0, x_0, \ldots)$.

Conseguimos então achar um esquema-grupo afim com as propriedades procuradas; falta provar que ele permite classificar os esquemas-grupos abelianos finitos.

Corolário 6.1.11. *Temos as propriedades dos mapas em $W \coloneqq W_{\mathbb{F}_p}$:*

(a) $F(x_0, x_1, \ldots) = (x_0^p, x_1^p, \ldots)$ é endomorfismo do esquema-anel W;

(b) $V(x_0, x_1, \ldots) = (0, x_0, x_1, \ldots)$ é endomorfismo do esquema-grupo abeliano W;

(c) $V(Fx) = F(Vx) = p \cdot x = (0, x_0^p, x_1^p, \ldots)$;

(d) $x \cdot Vy = V(Fx \cdot y)$.

Demonstração. Resta só (d). Primeiro, se $y = Fz$, vale

$$x \cdot Vy = x \cdot V(Fz) = x \cdot p \cdot z = p \cdot x \cdot z = V(F(x \cdot z)) = V(Fx \cdot Fz) = V(Fx \cdot y).$$

Para x fixo, os homomorfismos (aditivos) $y \mapsto x \cdot Vy$ e $y \mapsto V(Fx \cdot y)$ coincidem na imagem de $z \mapsto Fz$ (que é epimorfismo), logo coincidem para qualquer y. □

6.1.4 Os ideais de $W(k)$

Sendo k corpo perfeito de característica p, se $x, y \in W(k) \smallsetminus 0$, há mínimos i e j com $x_i, y_j \neq 0$, logo $x = V^i X$ e $y = V^j Y$ com $X_0, Y_0 \neq 0$. Vale: $x \cdot y = x \cdot V^j Y =$

$V\,(Fx \cdot V^{j-1}Y) = \cdots = V^j(F^j x \cdot Y) = V^j(V^i F^j X \cdot Y) = \cdots = V^{i+j}(F^j X \cdot F^i Y)$, e $(F^j X \cdot F^i Y)_0 = (X_0)^{p^j} \cdot (Y_0)^{p^i} \neq 0$; em particular, $x \cdot y \neq 0$. Mais detalhes:

Lema 6.1.12. *Se k é corpo perfeito de característica p, o anel $W(k)$ é domínio comutativo de ideais principais, cujos ideais são precisamente $\langle p^0\rangle \supsetneq \langle p^1\rangle \supsetneq \cdots \supsetneq \langle 0\rangle$ (e assim dito um "domínio de valoração discreta"). Em particular, $\frac{W(k)}{p^i \cdot W(k)}$ é $W(k)$-módulo de comprimento i.*

Demonstração. Acima se provou que $W(k)$ é domínio. Seja $I \subseteq W(k)$ ideal não nulo. Para cada $x \in I \smallsetminus 0$ há i mínimo com $x_i \neq 0$; há $x \in I \smallsetminus 0$ cujo i atinge o valor mínimo dentre as opções em $I \smallsetminus 0$. Vale $x = p^i \cdot y$ onde $y = (x_i^{1/p^i}, x_{i+1}^{1/p^i}, \ldots)$ (de k ser perfeito), assim $y_0 \neq 0$; e também $I \subseteq \langle p^i\rangle$.

Se mostrarmos que y é inversível, concluiremos que $\langle p^i\rangle \subseteq I$. Vale $y = (y_0, 0, \ldots) \cdot z$ onde $z \coloneqq (y_0^{-p^0} y_0, y_0^{-p^1} y_1, \ldots)$, logo $(1-z)_0 = 0$, logo a série $1 + (1-z) + (1-z)^2 + \cdots$ converge (pois a i-ésima parcela $(1-z)^i$ estará em $\langle p^i\rangle$, isto é, são nulas as i primeiras componentes), e dá o inverso de $1-(1-z)$; logo, z é inversível, e $y^{-1} = (y_0^{-1}, 0, \ldots) \cdot z^{-1}$.

Enfim, o $W(k)$-módulo $\frac{W(k)}{p^i \cdot W(k)}$ tem somente os submódulos $\frac{\langle p^i\rangle}{\langle p^i\rangle} \subsetneq \frac{\langle p^{i-1}\rangle}{\langle p^i\rangle} \subsetneq \cdots \subsetneq \frac{\langle p^0\rangle}{\langle p^i\rangle}$, que formam cadeia de comprimento i. □

6.2 Pareamento de vetores de Witt

Abrevie: $T_n^m(R) \coloneqq \{\overline{x} \in W(R) \mid \forall_{i \geq n} x_i = 0, \quad \forall_{i<n} x_i^{p^m} = 0\}$.

Lema 6.2.1. *Existem funções A, B, C, D tais que, para quaisquer $m, n \geq 1$ e qualquer anel R:*

(a) $T_n^m(R) \pm T_n^m(R) \subseteq T_{B(n)}^{A(m,n)}(R)$;
(b) $T_n^m(R) \cdot W(R) \subseteq T_{D(n)}^{C(m,n)}(R)$.
Em particular, $\widehat{W}(R) \coloneqq \bigcup_{m,n} T_n^m(R)$ é ideal de $W(R)$.

Demonstração. Lembrar que $(\pm), (\cdot)$ são as únicas operações naturais em W tais que para cada anel R vale

$$\Phi_i(x \pm y) = \Phi_i(x) \pm \Phi_i(y),\ \Phi_i(xy) = \Phi_i(x)\Phi_i(y),\ x, y \in W(R),$$

onde $\Phi_{i+1}(x) = p^{i+1} x_{i+1} + \Phi_i(x^\sigma)$.

(a) Damos um "peso" a cada monômio em $\mathbb{Z}[x_0, y_0, \ldots]$:

$$\left|\prod_{i\geq 0}(x_i^{e_i} y_i^{f_i})\right| = \sum_{i\geq 0}\left(e_i\,|x_i| + f_i\,|y_i|\right),\ |x_i| \coloneqq |y_i| \coloneqq p^i.$$

Um polinômio em $\mathbb{Z}[x_0, y_0, \ldots]$ é "isobárico" de peso P quando é combinação $\mathbb{Z}$-linear de monômios de peso $= P$.

Em $s = x \pm y$, temos: $s_0 = x_0 \pm y_0$,

$$s_{i+1} = x_{i+1} \pm y_{i+1} + \frac{\Phi_i(x^\sigma) \pm \Phi_i(y^\sigma) - \Phi_i(s^\sigma)}{p^{i+1}}.$$

Disso, pode-se provar por indução que $s_i \in \mathbb{Z}[x_0, y_0, \ldots]$ é isobárico de peso p^i. (De fato se vale para $i = 0, \ldots, j$, vale que $\Phi_j(s^\sigma) = \sum_{i=0}^{j} p^i s_i^{p^{j-i+1}}$ é isobárico de peso $p^i \cdot p^{j-i+1} = p^{j+1}$, e as parcelas restantes acima também, logo a soma s_{j+1} também é isobárica de peso p^{j+1}.)

Então, se R é um anel e $x, y \in T_n^m(R)$, sendo $s \coloneqq x \pm y$, se $s_i^{p^N} \neq 0$, então seu peso $p^i \cdot p^N$ é no máximo

$$(p^m - 1) \cdot p^0 + \cdots + (p^m - 1) \cdot p^{n-1} < p^{m+n},$$

isto é, $i + N < m + n$. Então $T_n^m(R) \pm T_n^m(R) \subseteq T_{m+n}^{m+n}(R)$.

(b) A prova é similar, mas damos peso 0 a cada y_i. □

(Vale que $\widehat{W}$ é união de esquemas afins, mas não é esquema afim).

Lembremos a série de potências

$$E(x,t) \coloneqq \exp\left(-L(x,t)\right) = \exp\left(-\sum_{i\geq 0} \frac{\Phi_i(x)}{p^i} \cdot t^{p^i}\right),$$

cujos coeficientes estão em $\mathbb{Z}_{(p)}[x_0, x_1, \ldots]$. A parcela $\Phi_i(x)/p^i \cdot t^{p^i}$ tem grau em t igual a p^i e o coeficiente é um polinômio isobárico de peso p^i; logo, o coeficiente de t^d, $d \in \mathbb{N}$, em $E(x,t)$ é um polinômio isobárico de peso d.

Definição 6.2.2. Define-se operação $\langle , \rangle : \widehat{W} \times W \to I$ (onde $I(R) \coloneqq R$) por:

$$\langle x, y \rangle \coloneqq E\left(x \cdot y, t\right)\big|_{t=1}$$

(Avaliação em $t = 1$ faz sentido, pois o coeficiente de t^d será polinômio isobárico de peso d em $\mathbb{Z}[s_0, s_1, \ldots]$, $s \coloneqq x \cdot y$, que será nulo para $d \gg 0$, pois $s \in \widehat{W}$.)

Como $\Phi_i(x \pm y) = \Phi_i(x) \pm \Phi_i(y)$, vale $E(x + y, t) = E(x,t) \cdot E(y,t)$. Assim, $\langle x, y + y' \rangle = \langle x, y \rangle \cdot \langle x, y' \rangle$ e $\langle x + x', y \rangle = \langle x, y \rangle \cdot \langle x', y \rangle$; em particular, $\langle x, y \rangle \cdot \langle x, -y \rangle = \langle x, 0 \rangle = E(0,1) = 1$, logo cada $\langle x, y \rangle$ é inversível; então $\langle , \rangle : \widehat{W} \times W \to \boldsymbol{G_m}$.

Definição 6.2.3. Define-se o esquema-anel W_n^m como o núcleo de $F^m : W_n \to W_n$. (A álgebra de W_n^m é $k[X_0, \ldots, X_n]/(X_0^{p^m}, \ldots, X_n^{p^m})$, de dimensão p^{mn}.)

Lema 6.2.4. *Temos sequências exatas curtas:* $0 \to W_N^m \xrightarrow{v^n} W_{n+N}^m \xrightarrow{r} W_n^m \to 0$ *(onde* r *é projeção nas* n *primeiras componentes);* $0 \to W_n^m \xrightarrow{i} W_n^{m+M} \xrightarrow{f^m} W_n^M \to 0$.

Demonstração. $W_n^{m+M} \xrightarrow{f^m} W_n^M$ é epimorfismo porque seu mapa de Hopf é $k[X_{[n]}]/(X_{[n]}^{p^M}) \to k[X_{[n]}]/(X_{[n]}^{p^{m+M}})$, $X_i \mapsto X_i^{p^m}$, que é monomorfismo. O resto, por elementos generalizados. □

Do corolário 6.1.11, vale $\langle x, Vy\rangle = E(x \cdot Vy, 1) = E(V(Fx \cdot y), 1) = E(Fx \cdot y, 1^p) = \langle Fx, y\rangle$. Então, se $F^n x = 0$ e $\forall_{i<n} y_i = z_i$, vale $y - z =: V^n w$, e $\langle x, y\rangle / \langle x, z\rangle = \langle x, y - z\rangle = \langle x, V^n w\rangle = \langle F^n x, w\rangle = \langle 0, w\rangle = 1$. Logo também há $\langle , \rangle : \widehat{W}^n \times W_n \to \boldsymbol{G_m}$, onde $\widehat{W}^n := \mathrm{nuc}(F^n : \widehat{W} \to \widehat{W})$. Similarmente, há $\langle , \rangle : \widehat{W}_m \times W^m \to \boldsymbol{G_m}$ e $\langle , \rangle : W_m^n \times W_n^m \to \boldsymbol{G_m}$.

6.2.1 Esquemas formais

Definição 6.2.5. Define-se o "functor dos elementos quase de grupo" $\mathrm{Sp}^* : \mathsf{CoMonAb}(k\text{−}\mathsf{Vect}, \otimes) \to \mathsf{Conj}^{k-\mathsf{Alg}}$ por:

$$\mathrm{Sp}^*(C)(R) := \{a \in C \otimes_k R \mid \epsilon_{C\otimes_k R}(a) = 1_R,\ \Delta_{C\otimes_k R}(a) = a \otimes_R a\}$$

Lema 6.2.6. Sp^* *é functor pleno fiel. (Os functores isomorfos a membros da imagem de* Sp^* *serão ditos "esquemas formais").*

Demonstração. Como na prova do lema 4.3.6, se C é coálgebra cocomutativa de dimensão finita, $\mathrm{Sp}^*(C)(R) \cong k\text{−}\mathsf{Alg}(C^*, R)$ por meio de $\Phi(\sum a \otimes r) := (f \mapsto \sum fa \cdot r)$. Notar $\Phi((H \otimes 1)(\sum a \otimes r)) = \Phi(\sum Ha \otimes r) = (f \mapsto \sum f(Ha) \cdot r) = \Phi(\sum a \otimes r) \circ (\circ H)$.

Então dadas C, D coálgebras cocomutativas quaisquer, que são uniões direcionadas de suas respectivas subcoálgebras de dimensões finitas C_i, D_j, vale que $\mathrm{Sp}^* C$ é união direcionada dos $\mathrm{Sp}^* C_i$, e $\mathsf{Conj}^{k-\mathsf{Alg}}(\mathrm{Sp}^* C, \mathrm{Sp}^* D) \cong \lim_i \mathsf{Conj}^{k-\mathsf{Alg}}(\mathrm{Sp}^* C_i, \mathrm{Sp}^* D) \cong \lim_i \mathsf{Conj}^{k-\mathsf{Alg}}(k\text{−}\mathsf{Alg}(C_i^*,), \mathrm{Sp}^* D)$, que por Yoneda é isomorfo a $\lim_i \mathrm{Sp}^* D(C_i^*)$, e este é isomorfo a $\lim_i \mathrm{co}\lim_j \mathrm{Sp}^* D_j(C_i^*) \cong \lim_i \mathrm{co}\lim_j k\text{−}\mathsf{Alg}(D_j^*, C_i^*) \cong \lim_i \mathrm{co}\lim_j \mathsf{CoMonAb}(k\text{−}\mathsf{Vect}, \otimes)(C_i, D_j) \cong \mathsf{CoMonAb}(k\text{−}\mathsf{Vect}, \otimes)(C, D)$. E o mapa

$$\mathsf{CoMonAb}(k\text{−}\mathsf{Vect}, \otimes)(C, D) \to \mathsf{Conj}^{k-\mathsf{Alg}}(\mathrm{Sp}^* C, \mathrm{Sp}^* D)$$

leva $f : C \to D$ a: $f_i := (f \restriction C_i) : C_i \to D_{(\dots)}$, $(\circ f_i) : D_{(\dots)}^* \to C_i^*$, $\Phi^{-1}(\circ f_i) \in \mathrm{Sp}^* D_{(\dots)}(C_i^*)$, $x \in \mathrm{Sp}^* C_i(R) \mapsto (1 \otimes \Phi x)\big(\Phi^{-1}(\circ f_i)\big) \in \mathrm{Sp}^* D_{(\dots)}(R)$, que é igual a $x \mapsto \Phi^{-1}\big(\Phi x \circ (\circ f_i)\big) = (f_i \otimes 1)(x) = \mathrm{Sp}^*(f)(x)$. Portanto, Sp^* é pleno fiel. □

Lema 6.2.7. *A categoria* $\mathsf{CoMonAb}(k\text{−}\mathsf{Vect}, \otimes)$ *tem objeto terminal* k*, e produtos são dados por produto tensorial, com projeções* $\pi_0 : C_0 \otimes C_1 \to C_0$ *e* $\pi_1 : C_0 \otimes C_1 \to C_1$*,* $\pi_0 := \langle 1, \epsilon_{C_1}\rangle$ *e* $\pi_1 := \langle \epsilon_{C_0}, 1\rangle$*.*

Demonstração. $C_0 \otimes C_1$ tem operações: $\epsilon(c_0 \otimes c_1) := \epsilon_{C_0} c_0 \cdot \epsilon_{C_1} c_1$; $\Delta(c_0 \otimes c_1) := T(\Delta_{C_0} c_0 \otimes \Delta_{C_1} c_1)$, onde $T((a_0 \otimes b_0) \otimes (a_1 \otimes b_1)) := (a_0 \otimes a_1) \otimes (b_0 \otimes b_1)$. (Similar ao coproduto de

álgebras de Hopf). O mapa π_0 é morfismo de coálgebras: $\epsilon_{C_0}(\pi_0(c_0 \otimes c_1)) = \epsilon_{C_0}(c_0 \cdot \epsilon_{C_0} c_1) = \epsilon(c_0 \otimes c_1)$; $(\pi_0 \otimes \pi_0)(\Delta(c_0 \otimes c_1)) = (\pi_0 \otimes \pi_0)(T(\Delta_{C_0} c_0 \otimes \Delta_{C_1} c_1)) = P(\Delta_{C_0} c_0 \otimes \Delta_{C_1} c_1)$, onde $P((a_0 \otimes b_0) \otimes (a_1 \otimes b_1)) \coloneqq a_0 \otimes b_0 \cdot \epsilon a_1 \cdot \epsilon b_1$, logo $(\pi_0 \otimes \pi_0)(\Delta(c_0 \otimes c_1)) = \Delta_{C_0} c_0 \cdot \langle \epsilon, \epsilon \rangle (\Delta_{C_1} c_1) = \Delta_{C_0}(\pi_0 c_0)$. E π_1 similarmente.

Resta a propriedade universal. Dados morfismos de coálgebras $f : D \to C_0$ e $g : D \to C_1$, define-se $h : D \to C_0 \otimes C_1$, $h \coloneqq (f \otimes g) \circ \Delta_D$; é morfismo de coálgebras porque $\epsilon \circ h = \langle \epsilon \circ f, \epsilon \circ g \rangle \circ \Delta = \langle \epsilon, \epsilon \rangle \circ \Delta = \epsilon$, e $\Delta \circ h = T \circ (\Delta_{C_0} \otimes \Delta_{C_1}) \circ (f \otimes g) \circ \Delta_D = T \circ ((f \otimes f) \circ \Delta_D \otimes (g \otimes g) \circ \Delta_D) \circ \Delta_D = (f \otimes g \otimes f \otimes g) \circ T \circ (\Delta_D \otimes \Delta_D) \circ \Delta_D \overset{*}{=} (h \otimes h) \circ \Delta_D$ onde $*$ usa cocomutatividade; assim, $\pi_0 \circ h = \langle f, \epsilon \cdot g \rangle \circ \Delta_D = f$, e similarmente $\pi_1 \circ h = g$. E se $h' : D \to C_0 \otimes C_1$ é outro morfismo de coálgebras com $\pi_0 \circ h' = f$ e $\pi_1 \circ h' = g$, então, $h = (\pi_0 \otimes \pi_1) \circ (h' \otimes h') \circ \Delta_D = (\pi_0 \otimes \pi_1) \circ \Delta_{C_0 \otimes C_1} \otimes h' = h'$ de $(\pi_0 \otimes \pi_1) \circ \Delta_{C_0 \otimes C_1} = (\pi_0 \otimes \pi_1) \circ T \circ (\Delta_{C_0} \otimes \Delta_{C_1}) = (\langle 1, \epsilon \rangle \otimes \langle \epsilon, 1 \rangle) \circ (\Delta_{C_0} \otimes \Delta_{C_1}) = 1 \otimes 1$. □

Lema 6.2.8. $\underline{\mathrm{Hom}}(, \boldsymbol{G_m})$ *é antiequivalência da categoria dos esquemas-grupos afins abelianos à categoria dos esquemas-grupos formais abelianos. (Em particular, a categoria dos esquemas-grupos formais abelianos também é abeliana).*

Demonstração. Vale $\underline{\mathrm{Hom}}(G, \boldsymbol{G_m})(R) = \mathsf{CoAb}(k\text{−}\mathsf{Alg})(k[X, X^{-1}], A_G \otimes R) = \mathrm{Sp}^*(A_G)(R)$. Já vimos Sp* ser equivalência da categoria $\mathsf{CoMonAb}(k\text{−}\mathsf{Vect}, \otimes)$ à categoria dos esquemas formais. Logo, Sp* induz equivalência entre as respectivas categoria de objetos-grupos abelianos. Um objeto-grupo abeliano na categoria dos esquemas formais é o mesmo que um esquema-grupo formal abeliano. Resta provar que um objeto-grupo abeliano em $\mathsf{CoMonAb}(k\text{−}\mathsf{Vect}, \otimes)$ é o mesmo que uma k-álgebra de Hopf cocomutativa.

Um objeto-monoide abeliano em $\mathsf{CoMonAb}(k\text{−}\mathsf{Vect}, \otimes)$ consiste duma k-coálgebra cocomutativa C, junto a lineares $u : k \to C$ e $m : C \otimes C \to C$, com: u e m são mapas de coálgebras (isto é, $\epsilon(u1) = 1$, $\epsilon \circ m = \langle \epsilon, \epsilon \rangle$, $\Delta(u1) = u1 \otimes u1$, $\Delta \circ m = (m \otimes m) \circ T \circ (\Delta \otimes \Delta)$); $m \circ \tau = m$ (onde $\tau(a \otimes b) \coloneqq b \otimes a$); $m \circ (u \circ \epsilon \otimes 1) \otimes \Delta_C = 1_C$; $m \circ (m \otimes 1_C) = m \circ (1_C \otimes m)$. Isso é o mesmo que uma k-álgebra (comutativa unitária) com produto m, e homomorfismos de álgebras ϵ e Δ satisfazendo as condições de coálgebra. E um objeto-grupo abeliano em $\mathsf{CoMonAb}(k\text{−}\mathsf{Vect}, \otimes)$ tem adicionalmente linear $S : C \to C$ com: S mapa de coálgebra (isto é, $\epsilon \circ S = \epsilon$ e $\Delta \circ S = (S \otimes S) \circ \Delta$); e $m \circ (S \otimes 1) \circ \Delta = u \circ \epsilon$ (isto é, $\langle S, 1 \rangle \circ \Delta = \epsilon$, abreviando $1 \coloneqq u1$ e $(\cdot) \coloneqq m$). Em particular, $\langle S, 1 \rangle (\Delta 1) = \epsilon 1$, logo $S1 = 1$. E por propriedades de objetos-grupos abelianos, vale $m \circ (S \otimes S) = S \circ m$, logo $\forall_{a,b} S(a \cdot b) = Sa \cdot Sb$. Portanto, $\mathsf{Ab}(\mathsf{CoMonAb}(k\text{−}\mathsf{Vect}, \otimes)) \cong \mathsf{CoAb}(k\text{−}\mathsf{Alg})$. □

Observação 6.2.9. Vale $\underline{\mathrm{Hom}}(G \oplus H, \boldsymbol{G_m}) \cong \underline{\mathrm{Hom}}(G, \boldsymbol{G_m}) \oplus \underline{\mathrm{Hom}}(H, \boldsymbol{G_m})$. Logo os produtos finitos de esquemas-grupos formais abelianos são também as somas finitas. E, dado $\phi : G \to H$, $\underline{\mathrm{Hom}}(\mathrm{conuc}\, \phi, \boldsymbol{G_m})(R) \cong \mathrm{Sp}^*(A_{\mathrm{conuc}\, \phi})(R) = \mathrm{Sp}^*(A_H)(R) \cap (A_{\mathrm{conuc}\, \phi} \otimes R)$. E, dado $v \in \mathrm{nuc}(\mathrm{Sp}^*\, \phi' : \mathrm{Sp}^*\, A_H(R) \to \mathrm{Sp}^*\, A_G(R))$, vale $(\phi'_R \otimes_R 1)(\Delta_{A_H \otimes R}(v)) = (\phi' \otimes_R 1)(v \otimes v) = \phi' v \otimes_R$

$v = 1_R \otimes_R v$, logo $v \in A_{\operatorname{conuc}\phi} \otimes R$. Então, $\underline{\operatorname{Hom}}(\operatorname{conuc}\phi, \boldsymbol{G_m})(R) \cong \operatorname{nuc}(\operatorname{Sp}^*\phi' : \operatorname{Sp}^* A_H(R) \to \operatorname{Sp}^* A_G(R))$, isto é, os núcleos de esquemas-grupos formais abelianos são precisamente os núcleos componenciais. Combinando os dois, os limites finitos de esquemas-grupos formais abelianos são os mesmos de functores.

Observação 6.2.10. Se $\phi : G \to H$ é morfismo de esquemas-grupos afins abelianos finitos, é em particular de esquemas-grupos formais abelianos, equivale a $\underline{\operatorname{Hom}}(, \boldsymbol{G_m})(G^* \xrightarrow{\phi^*} H^*)$, e assim $\phi : G \to H$ é mônico, épico, etc., na categoria dos esquemas-grupos formais abelianos sse $G^* \xrightarrow{\phi^*} H^*$ é épico, mônico, etc., na categoria dos esquemas-grupos afins abelianos, sse $\phi : G \to H$ é mônico, épico, etc., na categoria dos esquemas-grupos afins (finitos) abelianos.

6.2.2 Duais de W_n^m, W_n e W

Lema 6.2.11. *Há isomorfismos* $W_m^1 \cong (W_1^m)^* \cong \underline{\operatorname{Hom}}(W_1^m, \boldsymbol{G_m})$ *e* $\widehat{W}^1 \cong \underline{\operatorname{Hom}}(W_1, \boldsymbol{G_m})$ *dados por* $\langle , \rangle$.

Demonstração. (De (Demazure e Gabriel, 1970) II§2n2.6, V§4n4.5) Os mapas são $\phi_m : W_m^1 \to \underline{\operatorname{Hom}}(W_1^m, \boldsymbol{G_m})$, $\phi_R(x) := (R' \in R\text{–}\mathsf{Alg}) \mapsto y \mapsto \langle W_m^1(\iota_{R\to R'})x, y\rangle$, e similar $\phi_\infty : \widehat{W}^1 \to \underline{\operatorname{Hom}}(W_1, \boldsymbol{G_m})$. Para $m \in \mathbb{N} \cup \{\infty\}$, vale $\phi_m(x)_{R'}(y) = E(x \cdot (y, 0, \ldots), 1) = E((x_0 \cdot y, x_1 \cdot y^p, \ldots), 1)$ pelo fato 6.1.7. A fórmula $E(\vec{z}, t) = \exp(-\sum_{i\geq 0} S(z_i \cdot t^{p^i}))$ vale em característica zero; logo, denotando por $(\cdots)_{<p}$ a série de potências obtida removendo termos de graus $\geq p$, vale que $E(\vec{z}, t) - \exp_{<p}(-\sum_{i\geq 0} S_{<p}(z_i \cdot t^{p^i}))$ é série de potências em t onde cada coeficiente é múltiplo dalgum z_i^p. As séries de potências $\exp_{<p}$ e $S_{<p}$ podem ser usadas em característica p. Então, como $x \in W_m^1$ ou $x \in \widehat{W}^1$ implica cada $x_i^p = 0$, $\phi_m(x)_{R'}(y) = \exp_{<p}(-\sum_{i\geq 0} x_i \cdot y^{p^i})$. Também, sendo $L(X) := \log(1+X) = \sum_{i\geq 1}(-1)^{i+1}/i \cdot X^i$, como $L(\exp X - 1) = X$, $L_{<p}(\exp_{<p} X - 1) - X$ só tem termos de graus $\geq p$. Então, $L_{<p}(\phi_m(x)_{R'}(y) - 1) = -\sum_{i\geq 0} x_i \cdot y^{p^i}$. Em particular, para $R' := R[Y]/(Y^{p^m})$ (ou $R' := R[Y]$ para $m = \infty$), vale $Y \in W_1^m(R')$, e $\phi_m(x)_{R'}(Y) = 1 \implies L_{<p}(\phi_m(x)_{R'}(Y) - 1) = 0 \implies \forall_{0\leq i<m} x_i = 0$. Então ϕ_m é componencialmente injetivo.

Cada elemento $\psi \in \underline{\operatorname{Hom}}(W_1^m, \boldsymbol{G_m})(R)$, para $m \in \mathbb{N} \cup \{\infty\}$, é dado por elemento quase de grupo de $A_{W_1^m} \otimes R$, isto é, elemento $\sum_{i<p^m} X^i \otimes r_i$ com $r_0 = 1$ e $\sum_{i<p^m}(X \otimes 1 + 1 \otimes X)^i \otimes r_i = \sum_{i,j<p^m}(X^i \otimes X^j) \otimes (r_i \cdot r_j)$; isto é, $r_0 = 1$ e $\forall_{i,j} r_i \cdot r_j = \binom{i+j}{i} \cdot r_{i+j}$. Por indução, pode-se provar que:

$$r_{i_1} \cdot \ldots \cdot r_{i_l} = \binom{i_1 + i_2}{i_1} \cdot \ldots \cdot \binom{i_1 + \cdots + i_l}{i_1 + \cdots + i_{l-1}} \cdot r_{i_1+\cdots+i_l} = \binom{i_1 + \cdots + i_l}{i_1, \ldots, i_l} \cdot r_{i_1+\cdots+i_l}.$$

Denota-se por $\nu_p(\cdots)$ o número de fatores p na fatoração dum inteiro. Então, para cada $i < p^m$, escrito em base p, $i = \sum_{j<m} c_j \cdot p^j$, $0 \leq c_j < p$, vale:

$$\binom{i}{c_0 \cdot p^0, c_1 \cdot p^1, \ldots} \cdot r_i = r_{c_0 \cdot p^0} \cdot r_{c_1 \cdot p^1} \cdot \ldots,$$

$$\nu_p\binom{i}{c_0\cdot p^0, c_1\cdot p^1, \ldots} = \nu_p(i!) - \sum_j \nu((c_j\cdot p^j)!)$$
$$= \sum_{l\geq 1}\Big(\left\lfloor \frac{i}{p^l}\right\rfloor - \sum_j \left\lfloor \frac{c_j\cdot p^j}{p^l}\right\rfloor\Big) = \sum_{l\geq 1}\Big(\sum_{j\geq l} c_j\cdot p^{j-l} - \sum_{j\geq l} c_j\cdot p^{j-l}\Big) = 0,$$

de $c_j < p$, assim este coeficiente multinomial é coprimo a p. Também,

$$\binom{c_j\cdot p^j}{p^j,\ldots,p^j}\cdot r_{c_j\cdot p^j} = r_{p^j}^{c_j},$$

$$\nu_p\binom{c_j\cdot p^j}{p^j,\ldots,p^j} = \nu_p((c_j\cdot p^j)!) - c_j\cdot\nu_p(p^j!) = 0,$$

logo este coeficiente multinomial também é coprimo a p. Então, lembrando que a característica é p, $r_i = C(i)\cdot r_{p^0}^{c_0}\cdot r_{p^1}^{c_1}\cdot\ldots$, onde:

$$C(i) \coloneqq \binom{i}{c_0\cdot p^0, c_1\cdot p^1,\ldots}^{-1}\cdot\prod_j\binom{c_j\cdot p^j}{p^j,\ldots,p^j}^{-1} = \frac{(p^0!)^{c_0}\cdot(p^1!)^{c_1}\cdot\ldots}{i!}$$

Também, $\nu_p\binom{p\cdot j}{j,\ldots,j} = \sum_{l\geq 1}(\lfloor j/p^{l-1}\rfloor - p\cdot\lfloor j/p^l\rfloor) > 0$ porque cada parcela é ≥ 0 e existe l com $p^{l-1}\leq j < p^l$, logo $\lfloor j/p^{l-1}\rfloor - p\cdot\lfloor j/p^l\rfloor > 0$; assim, $r_j^p = \binom{p\cdot j}{j,\ldots,j}\cdot r_{p\cdot j} = 0$, isto é, $r_j\in W_m^1(R)$ ou $\in\widehat{W}^1(R)$. Então:

$$\begin{aligned}
C(i) &= \prod_{j\geq 0}^{i\geq p^j}\frac{(p^j)!^{c_j}}{\prod_{l=1}^{c_j\cdot p^j}(l+\sum_{r>j}c_r\cdot p^r)}\\
&= \prod_{j\geq 0}^{i\geq p^j}\prod_{l=1}^{c_j\cdot p^j}\frac{l-\lfloor(l-1)/p^j\rfloor\cdot p^j}{l+\sum_{r>j}c_r\cdot p^r}\\
&= \prod_{j\geq 0}^{i\geq p^j}\prod_{e=0}^{j}\prod_{1\leq d\leq c_j\cdot p^{j-e}}^{d\perp p}\frac{p^e\cdot d-\lfloor(p^e\cdot d-1)/p^j\rfloor\cdot p^j}{p^e\cdot d+\sum_{r>j}c_r\cdot p^r}\\
&= \prod_{j\geq 0}^{i\geq p^j}\prod_{e=0}^{j}\prod_{1\leq d\leq c_j\cdot p^{j-e}}^{d\perp p}\frac{d-\lfloor(p^e\cdot d-1)/p^j\rfloor\cdot p^{j-e}}{d+\sum_{r>j}c_r\cdot p^{r-e}}\\
&= \prod_{j\geq 0}^{i\geq p^j}\Big(\prod_{e=0}^{j-1}\prod_d\frac{d+(\cdots)\cdot p}{d+(\cdots)\cdot p}\Big)\cdot\prod_{d=1}^{c_j}\frac{1}{d+(\cdots)\cdot p},
\end{aligned}$$

$$C(i)\equiv\prod_{j\geq 0}^{i\geq p^j}(c_j!)^{-1}\pmod p,$$

$$\phi_m(-r_{p^0}, -r_{p^1}, \ldots)_{R'}(y) = \exp_{<p}(\sum_{j\geq 0} r_{p^j} \cdot y^{p^j}) = \prod_{j\geq 0} \exp_{<p}(r_{p^j} \cdot y^{p^j})$$
$$= \prod_{j\geq 0} \sum_{c<p} (r_{p^j} \cdot y^{p^j})^c / c! = \sum_{i\geq 0}^{i=c_0\cdot p^0+\cdots} y^i \cdot \frac{r_{p^0}^{c_0} \cdot r_{p^1}^{c_1} \cdot \ldots}{c_0! \cdot c_1! \cdot \ldots} = \sum_{i\geq 0}^{i=c_0\cdot p^0+\cdots} y^i \cdot \frac{r_i}{C(i) \cdot c_0! \cdot c_1! \cdot \ldots}$$
$$= \sum_{i\geq 0} y^i \cdot r_i = \psi_{R'}(y).$$

Então ϕ_m é componencialmente sobrejetivo, logo isomorfismo. □

Teorema 6.2.12. *Existem isomorfismos* $W_m^n \cong (W_n^m)^*$ *e* $\widehat{W}^n \cong \underline{\mathrm{Hom}}(W_n, \boldsymbol{G_m})$ *dados por* $\langle , \rangle$.

Demonstração. Faz-se indução em n. Caso $n = 0$ trivial. Caso $n = 1$ pelo lema acima. Supõe-se agora $n \geq 2$. Há diagramas de esquemas-grupos afins abelianos

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_m^1 & \xrightarrow{i} & W_m^n & \xrightarrow{f} & W_m^{n-1} & \longrightarrow & 0 \\ & & \phi\downarrow\sim & & \phi\downarrow & & \phi\downarrow\sim & & \\ 0 & \longrightarrow & (W_1^m)^* & \xrightarrow[r^*]{} & (W_n^m)^* & \xrightarrow[v^*]{} & (W_{n-1}^m)^* & \longrightarrow & 0 \end{array}$$

A primeira linha é exata por definição de W_m^1. A segunda linha é exata porque dualização é antiequivalência. O diagrama comuta porque $\langle ix, y\rangle = \langle x, ry\rangle$ e $\langle fx, y\rangle = \langle x, vy\rangle$. Como os mapas verticais das pontas são isomorfismos, por lema de homologia o do meio é isomorfismo.

A prova de $\widehat{W}^n \cong \underline{\mathrm{Hom}}(W_n, \boldsymbol{G_m})$ necessita das adaptações: a categoria dos esquemas-grupos formais abelianos é abeliana pelo lema 6.2.8; vale $W_m^n \cong (W_n^m)^* \cong \mathrm{Sp}^*(A_{W_n^m})$, logo $\mathrm{Sp}^*(\mathrm{co\,lim}_m A_{W_n^m}) \cong \bigcup_n W_m^n = \widehat{W}^n$ é esquema formal, e tem operações de grupo naturais; $\widehat{W}^1 \to \widehat{W}^n$ é componencialmente injetivo, logo é mônico; $\widehat{W}^1$ é núcleo componencial de $\widehat{W}^n \to \widehat{W}^{n-1}$, logo é o núcleo nessa categoria; e $f : \widehat{W}^n \to \widehat{W}^{n-1}$ é induzido dos mapas $f : W_m^n \to W_m^{n-1}$, que são épicos pois são duais (pela parte acima) aos mônicos $v : W_{n-1}^m \to W_n^m$; então a primeira linha é exata; a segunda linha $0 \to \underline{\mathrm{Hom}}(W_1, \boldsymbol{G_m}) \to \underline{\mathrm{Hom}}(W_n, \boldsymbol{G_m}) \to \underline{\mathrm{Hom}}(W_{n-1}, \boldsymbol{G_m}) \to 0$ é exata por $\underline{\mathrm{Hom}}(, \boldsymbol{G_m})$ ser antiequivalência aditiva, e $0 \to W_{n-1} \to W_n \to W_1 \to 0$ é exata. □

Corolário 6.2.13. *Existe isomorfismo* $\widehat{W} \cong \underline{\mathrm{Hom}}(W, \boldsymbol{G_m})$ *dado por* $\langle , \rangle$.

Demonstração. Vale $\underline{\mathrm{Hom}}(W_n, \boldsymbol{G_m}) \cong \widehat{W}^n$, W é limite de $\cdots \to W_1 \to W_0$, e como $\underline{\mathrm{Hom}}(, \boldsymbol{G_m})$ é antiequivalência, vale que $\underline{\mathrm{Hom}}(W, \boldsymbol{G_m})$ é colimite de $\widehat{W}^0 \to \widehat{W}^1 \cdots$, que é $\widehat{W}$. □

6.3 Anel de Dieudonné

Definição 6.3.1. Se k é corpo perfeito, define-se E como o $W(k)$-módulo esquerdo de base $\ldots, V^2, V^1, V^0 = 1 = F^0, F^1, F^2, \ldots$, e com operação de anel não necessariamente comutativo induzida por: (onde $(\xi_0, \xi_1, \ldots)^\sigma \coloneqq (\xi_0^p, \xi_1^p, \ldots)$) $F \cdot V = V \cdot F = p$, $\quad F \cdot (\xi \in W(k)) \cdot 1 = \xi^\sigma \cdot F$, $\quad V \cdot (\xi \in W(k)) \cdot 1 = \xi^{\sigma^{-1}} \cdot V$.

Denotamos $[a, x, b] \coloneqq \max(a, \min(b, x))$; e $\tau_i(\xi) \coloneqq (0^{(i-1)}, \xi, 0^{(\infty)})$ (única componente não nula possível é a i-ésima). Lembrar $\tau_0(\xi) \cdot \tau_0(\pi) = \tau_0(\xi \cdot \pi)$, logo $\tau_{i+j}(\xi^{p^{i+j}} \cdot \pi^{p^{i+j}}) = p^{i+j} \cdot \tau(\xi \cdot \pi) = \tau_i(\xi^{p^i}) \cdot \tau_j(\pi^{p^j})$; então $\tau_{i+j}(\xi^{p^j} \cdot \pi^{p^i}) = \tau_i(\xi) \cdot \tau_j(\pi)$ pois $\xi \mapsto \xi^{p^i}$ e $\pi \mapsto \pi^{p^j}$ são epimorfismos.

Lema 6.3.2. *Há isomorfismo* $\frac{E}{E \cdot V^n} \cong \mathrm{End}_{\mathsf{Ab}^{k-\mathsf{Alg}}}(W_n)$ *de* k*–álgebras.*

Demonstração. Tentamos definir $\Phi : E \to \mathrm{End}(W_n)$ por: $\Phi(\xi \cdot F^i)_{(R)}(w \in W_n(R)) \coloneqq \xi^{\sigma^{-n}} \cdot F^i w$; $\Phi(\xi \cdot V^i)_{(R)}(w) \coloneqq \xi^{\sigma^{-n}} \cdot V^i w$ (mais propriamente, restrinja $\xi^{\sigma^{-n}}$ a n componentes para multiplicar com elementos de $W_n(R)$). Até agora Φ é k–linear. Para mostrar multiplicativo, devemos provar $\Phi(\xi \cdot X_i \cdot \pi \cdot X_j) = \Phi(\xi \cdot X_i) \circ \Phi(\pi \cdot X_j)$, onde $X_i \coloneqq F^i$ (se $i \geq 0$) ou V^{-i} (se $i \leq 0$). Além dos casos triviais, resta provar: $\Phi(F) \circ \Phi(V) = \Phi(p) = \Phi(V) \circ \Phi(F)$, fácil; $\Phi(F) \circ \Phi(\xi) = \Phi(\xi^\sigma) \circ \Phi(F)$, que vem de $F(\xi \cdot w) = F\xi \cdot Fw$; $\Phi(V) \circ \Phi(\xi) = \Phi(\xi^{\sigma^{-1}}) \circ \Phi(V)$, que vem de $V(\xi \cdot w) = F^{-1}\xi \cdot Vw$ (corolário 6.1.11(d)).

Vemos $\Phi(V^n) = 0$. Vale $E \cdot V^n = \sum_{i \in \mathbb{Z}} W(k) \cdot X_i \cdot V^n = \sum_{i \in \mathbb{Z}} W(k) \cdot p^{[0,i,n]} \cdot X_{i-n}$; assim fácil ver que $E \cdot V^n$ é ideal. Logo, induz-se $\Phi : \frac{E}{E \cdot V^n} \to \mathrm{End}(W_n)$.

Prova-se por indução em n que $\Phi : \frac{E}{E \cdot V^n} \to \mathrm{End}(W_n)$ é injetivo. Caso $n = 0$ trivial.

Supor $n \geq 1$. Seja $[e] \in \frac{E}{E \cdot V^n}$ com $\Phi e = 0$; escreva $e \coloneqq \sum_j \xi^j \cdot X_j$. Como $E \cdot V^n = \sum_j W(k) \cdot p^{[0,j+n,n]} \cdot X_j$, e como $\xi^j = ((\xi^j)_{<[0,j+n,n]}, 0^{(\infty)}) + (0^{[0,j+n,n]}, (\xi^j)_{\geq [0,j+n,n]})$, onde a segunda parcela está em $W(k) \cdot p^{[0,j+n,n]}$, podemos supor que $(\xi^j)_{\geq [0,j+n,n]} = 0$ para cada j. Logo, $e = \sum_{1 \leq j < n} \xi^{-j} \cdot V^j + \sum_{j \geq 0} \xi^j \cdot F^j$, onde $\forall_{0 \leq j < n} \forall_{i \geq n-j} (\xi^{-j})_i = 0$ e $\forall_{j \geq 0} \forall_{i \geq n} (\xi^j)_i = 0$.

Por hipótese indutiva, como $\Phi^{[n::=n-1]} e = 0$, vale $e \in E \cdot V^{n-1}$; isto é, $\forall_{0 \leq j < n-1} \forall_{i < n-1-j} (\xi^{-j})_i = 0$ e $\forall_{j \geq 0} \forall_{i < n-1} (\xi^j)_i = 0$. Então, $\forall_{0 \leq j < n} \xi^{-j} = \tau_{n-1-j}((\xi^{-j})_{n-1-j})$ e $\forall_{j \geq 0} \xi^j = \tau_{n-1}((\xi^j)_{n-1})$; abrevie $\xi^j \coloneqq \tau_{(\ldots)}(\alpha_j)$.

Vale $e = \sum_{j=1}^{n-1} \tau_{n-1-j}(\alpha_{-j}) \cdot V^j + \sum_{j \geq 0} \tau_{n-1}(\alpha_j) \cdot F^j$. Sendo $R \coloneqq k[X]$, aplicamos $\Phi(e)$ a $\tau_0(X)$, obtendo $0 = \sum_{j=1}^{n-1} \tau_{n-1-j}(\alpha_{-j}^{p^{-n}}) \cdot \tau_j(X) + \sum_{j \geq 0} \tau_{n-1}(\alpha_j^{p^{-n}}) \cdot \tau_0(X^{p^j}) = \sum_{j=1}^{n-1} \tau_{n-1}(\alpha_{-j}^{p^{j-n}} \cdot X^{p^{n-1-j}}) + \sum_{j \geq 0} \tau_{n-1}(\alpha_j^{p^{-n}} \cdot X^{p^{j+n-1}})$; na componente $n-1$, temos $0 = \sum_{j=1}^{n-1} \alpha_{-j}^{p^j} \cdot X^{p^{n-1-j}} + \sum_{j \geq 0} \alpha_j \cdot X^{p^{j+n-1}}$, e como os $X^{p^{n-2}}, \ldots, X^{p^0}, X^{p^{n-1}}, X^{p^n}, \ldots$ são linearmente independentes, cada $\alpha_j = 0$, e $e = 0$.

Resta agora mostrar $\Phi : \frac{E}{E \cdot V^n} \to \mathrm{End}(W_n)$ sobrejetivo. Indução em n. Caso $n = 0$ trivial. Supor $n \geq 1$.

Seja $\phi \in \mathrm{End}(W_n)$. Seja $R \coloneqq k[X]$. Defina $\psi_i : R \to R$, $\psi_i X \coloneqq X^{p^i}$; por naturalidade, $\phi \circ W\psi_i = W\psi_i \circ \phi$, onde $W\psi_i = W_n\psi_i \coloneqq (r_0, \ldots) \mapsto (\psi_i r_0, \ldots)$. Notar $p^i \cdot \phi_R(\tau_0 X) = \phi_R(p^i \cdot \tau_0 X) = \phi_R(\tau_i X^{p^i}) = \phi_R(W\psi_i(\tau_i X)) = W\psi_i(\phi_R(\tau_i X))$; então as componentes $0, \ldots, i-1$ de $W\psi_i(\phi_R(\tau_i X))$ são nulas; como ψ_i é injetivo, as componentes de $0, \ldots, i-1$ de $\phi_R(\tau_i X)$ são nulas.

Logo, dada S álgebra qualquer, dado s na imagem de $v : W_{n-1}(S) \to W_n(S)$, sendo $\chi_i : R \to S$ com $\chi_i(X) \coloneqq s_i$, vale que o elemento $\phi_S(s) = \sum_{i\geq 1} \phi_S(\tau_i s_i) = \sum_{i\geq 1} \phi_S(\tau_i(\chi_i X)) = \sum_{i\geq 1} W\chi_i(\phi_R(\tau_i X))$ está na imagem de v. Se adicionalmente $\phi_R(\tau_0 X)$ está na imagem de v, então a imagem de cada ϕ_S está contida na imagem de v.

Agora seja $w \coloneqq \phi_{(R)}(\tau_0(X))$. O termo w_0 é um polinômio $f(X)$. Como $\tau_0(X+Y) - \tau_0(X) - \tau_0(Y)$ está na imagem de v, $\phi_{(R)}(\tau_0(X+Y)) - \phi_{(R)}(\tau_0 X) - \phi_{(R)}(\tau_0 Y)$ está na imagem de v; isto é, $f(X+Y) - f(X) - f(Y) = 0$. Escrevendo $f(X) \coloneqq \sum_{d\geq 0}^{r\perp p} c_{d,r} \cdot X^{r\cdot p^d}$, vale $f(X+Y) = \sum_{d\geq 0}^{r\perp p} c_{d,r} \cdot (X^{p^d} + Y^{p^d})^r = \sum_{d\geq 0}^{r\perp p} c_{d,r} \cdot \sum_{i=0}^{r} \binom{r}{i} \cdot X^{p^d\cdot i} \cdot Y^{p^d\cdot(r-i)}$; como $2 \leq r \perp p \implies \binom{r}{1} = r \neq 0 \in k$, necessariamente $c_{d,r} = 0$ se $2 \leq r \perp p$; logo $f(X) = \sum_{d\geq 0} c_{d,1} \cdot X^{p^d}$.

Escreva $e' \coloneqq \sum_{j\geq 0} \tau_0(c_{d,1}^{p^n}) \cdot F^j$; logo, $\Phi(e')(\tau_0 X) = \sum_{j\geq 0} \tau_0(c_{d,1} \cdot X^{p^j})$, cuja componente 0 é $\sum_{j\geq 0} c_{d,1} \cdot X^{p^j} = f(X) = w_0$. Então $\Phi(e') - \phi$ leva $\tau_0 X \in W_n(R)$ a elemento de imagem de v. Como vimos antes, $\Phi(e') - \phi$ deve fatorar-se unicamente $W_n \xrightarrow{\phi'} W_{n-1} \xrightarrow{v} W_n$. O mapa ϕ' leva imagens de V^{n-1} a imagens de $V^{n-1} : W_{n-1} \to W_{n-1}$, que se anularão; logo fatora-se como $W_n \xrightarrow{\pi} W_{n-1} \xrightarrow{\phi''} W_{n-1}$.

Por hipótese indutiva, existe e'' com $\Phi^{[n-1]}(e'') = \phi''$. Note que $v \circ \Phi^{[n-1]}(e'') = \Phi(e'') \circ v : W_{n-1} \to W_n$: pois e'' é soma dos $\xi \cdot X_i$, e $(v \circ \Phi^{[n-1]}(\xi \cdot X_i))(w) = v(\xi^{\sigma^{-(n-1)}} \cdot X_i w) = \xi^{\sigma^{-n}} \cdot v(X_i w) = \xi^{\sigma^{-n}} \cdot X_i(vw) = \Phi(\xi \cdot X_i)(vw)$. Então $\Phi(e'') \circ v = v \circ \phi'' : W_{n-1} \to W_n$.

Logo, $\phi = \Phi(e') - v \circ \phi'' \circ \pi = \Phi(e') - \Phi(e'') \circ v \circ \pi = \Phi(e') - \Phi(e'') \circ V = \Phi(e' - e'' \cdot V)$, como desejado. □

Observação 6.3.3. No lema acima, cada $W_n(R)$ recebe (naturalmente) E-ação. No meio da prova $v \circ \Phi^{[n-1]}(e'') = \Phi(e'') \circ v$, o que significa que cada $v : W_n(R) \to W_{n+1}(R)$ é E-linear.

Lema 6.3.4. *E é anel (não necessariamente comutativo) noetheriano (esquerdo); logo $\frac{E}{E\cdot V^n}$ também é noetheriano.*

Demonstração. O anel E é um quociente do anel R, cujos elementos são as somas $\sum_{i,j} (x_{i,j} \in W(k)) \cdot X^i \cdot Y^j$, onde X e Y são incógnitas que se comutam, e $X \cdot x = x^\sigma \cdot X$ e $Y \cdot x = x^{\sigma^{-1}} \cdot Y$; logo, basta provar R noetheriano. O subanel R_1 de R gerado por $W(k) \cup \{X\}$ é $W(k)[X]$ mas com a operação $X \cdot x = x^\sigma \cdot X$; mesmo assim, a prova do teorema da base de Hilbert pode ser repetida para dar que R_1 é noetheriano; similarmente, R é $R_1[Y]$ mas com a operação $Y \cdot (x \cdot X) = (x^{\sigma^{-1}} \cdot X) \cdot Y$, logo R é noetheriano. □

6.4 Em direção ao teorema de classificação

Definição 6.4.1. Definimos $M(G)$ (o "módulo de Dieudonné") como o colimite de E-módulos $\hom(G, W_0) \xrightarrow{v\circ} \hom(G, W_1) \to \hom(G, W_2) \to \cdots$.

(Notar que, como cada $W_{i-1} \to W_i$ é injetivo, cada $\hom(G, W_{i-1}) \to \hom(G, W_i)$ é injetivo, logo esse colimite é uma união).

Sejam as categorias: $\mathcal{C}$ a subcategoria dos esquemas-grupos afins abelianos G em que $\forall_{a \in \operatorname{nuc}\epsilon \subseteq A_G} \exists_n V^n a = 0 \in A_G^{(p)^n}$; $\mathcal{D}$ a subcategoria dos E–módulos em que $\forall_x \exists_n V^n \cdot x = 0$. (Notar que ambas as subcategorias são fechadas nos limites e colimites finitos). O objetivo será provar que M é equivalência $\mathcal{C}^\circ \to \mathcal{D}$, que se fará por partes.

Lema 6.4.2. *M define functor $\mathcal{C}^\circ \to \mathcal{D}$.*

Demonstração. Um elemento de MG é da forma $[f : G \to W_n]$; corresponde a mapa $g : A_{W_n} \to A_G$; o núcleo de $\epsilon : A_{W_n} \to k$ é finitamente gerado (sendo ideal de álgebra finitamente gerada), e sendo ξ_i, $1 \le i \le m$, os geradores, vale $g\xi_i \in \operatorname{nuc}\epsilon \subseteq A_G$; assim há $N \ge n$ com $V^N(g\xi_i) = 0$ para cada $1 \le i \le m$. Então, $V^N \circ g \restriction (\operatorname{nuc}\epsilon \subseteq A_{W_n}) = 0$, isto é, $V^N \circ g = (A_{W_n} \xrightarrow{\epsilon} k \xrightarrow{\sigma^p} k^{(p)^N} \to A_G^{(p)^N})$; logo, $f \circ V^N : G^{(p)^N} \to W_n$ é trivial; como V é natural, $V^N \circ f^{(p)^N} : G^{(p)^N} \to W_n^{(p)^N} \to W_n$ é trivial; como $W_n \cong W_n^{(p)^N}$, o mapa $(V^N \circ f)^{(p)^N} : G^{(p)^N} \to W_n^{(p)^N}$ é trivial; como $(\_)^{(p)^N}$ é functor fiel (verificar nas álgebras), $V^N \circ f : G \to W_n$ é trivial, logo $V^N \cdot [f] = 0$. □

Lema 6.4.3. *O functor M é exato esquerdo (isto é, leva colimites finitos de $\mathcal{C}$ a limites finitos de $\mathcal{D}$).*

Demonstração. Cada $\hom(\_, W_n)$ leva colimites finitos de $\mathcal{C}$ a limites finitos; e o colimite $\hom(\_, W_n) \to \hom(\_, W_{n+1}) \to \cdots$ é uma união, logo preserva esses limites finitos (porque preserva produtos finitos e mônicos). □

Lema 6.4.4. *Sendo $\{A_i\} \subseteq A$ a família das subálgebras de Hopf finitamente geradas, vale que $MG \cong \operatorname{co\,lim}_i MG_i$ onde este colimite é uma união direcionada.*

Demonstração. Como $A_i \to A_j \to A$ são injetivos, $G \to G_j \to G_i$ são epimorfismos, que M leva a monomorfismos (injetivos) $MG_i \to MG_j \to MG$. Também, $MG = \operatorname{co\,lim}_l \hom(A_{W_l}, A) \cong \operatorname{co\,lim}_{l,i} \hom(A_{W_l}, A_i) \cong \operatorname{co\,lim}_i MG_i$, porque cada A_{W_l} é finitamente gerada e porque colimites comutam com colimites. □

Lema 6.4.5. *Se $G \in \mathcal{C}$ é algébrico, há N tal que o canônico $\hom(G, W_N) \to MG$ é isomorfismo.*

Demonstração. Como A_G é finitamente gerada, $\operatorname{nuc}\epsilon \subseteq A_G$ é gerado por alguns $a_1, \ldots, a_m$; logo há N com cada $V^N a_i = 0$; e para cada $x \in \operatorname{nuc}\epsilon$; logo $V^N(\operatorname{nuc}\epsilon \subseteq A_G) = 0$. Então, se $f : G \to W_{N+M}$, vale $0 = f \circ V^N = V^N \circ f^{(p)^N} : G^{(p)^N} \to W_{N+M}^{(p)^N} \cong W_{N+M}$; logo $0 = V^N \circ f : G \to W_{N+M}$ como num lema anterior; logo, f fatora-se como $G \xrightarrow{f'} W_N \xrightarrow{v^M} V_{N+M}$; e assim $[f] \in MG$ é igual a $[f' \in \hom(G, W_N)] \in MG$. □

Lema 6.4.6. $MW_n \cong \frac{E}{E \cdot V^n}$.

Demonstração. Como na prova anterior, $MW_n \cong \hom(W_n, W_n)$, que vimos ser $\frac{E}{E \cdot V^n}$. □

Queremos também provar M exato direito, isto é, que M leva monomorfismos de $\mathcal{C}$ a epimorfismos (sobrejetivos) de $\mathcal{D}$. Assim, precisaremos saber dado $G \subseteq H$, quando mapas $H \to W_n$ podem ser estendidos a $G \to W_n$. Estudaremos as sequências exatas $0 \to W_n \to (\cdots) \to W_1 \to 0$ e veremos quando cindem (para haver mapas $(\cdots) \to W_n$).

Lema 6.4.7. *Seja mônico $\iota : G \to W_1$ (onde G é esquema-grupo afim abeliano). Então, para cada $n \geq 1$: (a) $\mathrm{Ext}^1(1, r^{n-1}) : \mathrm{Ext}^1(G, W_n) \to \mathrm{Ext}^1(G, W_1)$ é bijetivo; (b) $\mathrm{Ext}^1(\iota, 1) : \mathrm{Ext}^1(W_1, W_n) \to \mathrm{Ext}^1(G, W_n)$ é sobrejetivo; (c) $\mathrm{Ext}^1(W_1, W_n)$ é $k[F]$-módulo direito (onde $k[F] \subseteq E$ é o subanel gerado por $W(k) \cup \{F\}$), e é gerado por $e_n \coloneqq (W_n \xrightarrow{v} W_{n+1} \xrightarrow{r^n} W_1)$.*

Demonstração. (De Demazure e Gabriel (1970) V§1n2) Primeiro, em (c), a $k[F]$-ação direita (não esquerda) é dada por $X \mapsto \mathrm{Ext}^1(\Phi X, 1)$, onde lembramos $\Phi : E \to \mathrm{End}(W_1)$.

Faz-se indução em n. Consideremos primeiro $n \geq 2$, que é mais fácil.

Há exata $0 \to W_n \xrightarrow{v} W_{n+1} \xrightarrow{r^n} W_1 \to 0$, logo há diagrama comutativo

$$\begin{array}{ccccc} \mathrm{Ext}^1(G, W_n) & \longrightarrow & \mathrm{Ext}^1(G, W_{n+1}) & \longrightarrow & \mathrm{Ext}^1(G, W_1) \\ \uparrow & & \uparrow & & \uparrow \\ \mathrm{Ext}^1(W_1, W_n) & \xrightarrow{0} & \mathrm{Ext}^1(W_1, W_{n+1}) & \longrightarrow & \mathrm{Ext}^1(W_1, W_1) \end{array}$$

onde as linhas são exatas (lema 2.9.12, categoria dual), e os mapas verticais são $\mathrm{Ext}^1(\iota, 1)$. Vale $\mathrm{Ext}^1(1, v)(e_n) = 0 \in \mathrm{Ext}^1(W_1, W_{n+1})$, pelo lema 2.9.13. Os mapas horizontais $\mathrm{Ext}^1(1, \cdots)$ comutam com ação $\mathrm{Ext}^1(\Phi X, 1)$, logo são $k[F]$-lineares. Por hipótese indutiva em (c), então $\mathrm{Ext}^1(W_1, W_n) \to \mathrm{Ext}^1(W_1, W_{n+1})$ é nulo. No quadrado esquerdo, por hipótese indutiva em (b), $\mathrm{Ext}^1(W_1, W_n) \to \mathrm{Ext}^1(G, W_n)$ é sobrejetivo, o que implica $\mathrm{Ext}^1(G, W_n) \to \mathrm{Ext}^1(G, W_{n+1})$ nulo também. Por exatidão, $\mathrm{Ext}^1(1, r^n) : \mathrm{Ext}^1(G, W_{n+1}) \to \mathrm{Ext}^1(G, W_1)$ é injetivo. (Parte do item a)

Também, $\mathrm{Ext}^1(1, r^n)(e_{n+1}) \in \mathrm{Ext}^1(W_1, W_1)$ é calculado assim

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_{n+1} & \xrightarrow{v} & W_{n+2} & \xrightarrow{r^{n+1}} & W_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle R^n} & & \downarrow{\scriptstyle r^n} & & \| & & \\ 0 & \longrightarrow & W_1 & \xrightarrow{v} & W_2 & \xrightarrow{r} & W_1 & \longrightarrow & 0 \end{array}$$

(basta verificar diagrama comutativo e segunda linha exata) logo $\mathrm{Ext}^1(1, r^n)(e_{n+1}) = e_1$. Por hipótese indutiva (c, $n ::= 1$), $\mathrm{Ext}^1(W_1, W_{n+1}) \to \mathrm{Ext}^1(W_1, W_1)$ é sobrejetivo; e

é injetivo também porque $\mathrm{Ext}^1(W_1, W_n) \to \mathrm{Ext}^1(W_1, W_{n+1})$ é nulo; então, $\mathrm{Ext}^1(W_1, W_{n+1})$ também é $k[F]$-gerado por e_{n+1}. (Item c)

Então, no quadrado direito, a composição $\mathrm{Ext}^1(W_1, W_{n+1}) \to \mathrm{Ext}^1(W_1, W_1) \to \mathrm{Ext}^1(G, W_1)$ é sobrejetiva; assim também obtemos sobrejetivo $\mathrm{Ext}^1(G, W_{n+1}) \to \mathrm{Ext}^1(G, W_1)$, logo bijetivo. (Resto do item a) E assim o vertical do meio é sobrejetivo também. (Item b)

Resta agora o caso $n = 1$. Item (a) é trivial. Precisará de estudo mais detalhado de extensões, na próxima seção.

$\triangledown$

6.4.1 Extensões por W_1

Definição 6.4.8. Se $0 \to G \xrightarrow{f} H \xrightarrow{g} K \to 0$ é uma extensão de esquemas-grupos afins abelianos com uma seção natural (não necessariamente aditiva) $s : K \to H$ (isto é, $g \circ s = 1_K$) e com $s(0 \in K(R)) = 0$ para cada $R \in k\text{–}\mathsf{Alg}$, definimos (natural) $\kappa : K \times K \to G$ por: para cada k–álgebra R, e quaisquer $a, b \in K(R)$, como $g(s(a + b)) = g(s(a) + s(b))$, há único $\kappa(a, b)$ tal que $-s(a + b) + s(a) + s(b) = f(\kappa(a, b))$.

Definição 6.4.9. Dados esquemas-grupos afins abelianos G e K, definimos $Z^2(K, G)$ (os "2-cociclos" [normalizados simétricos]) como a família dos naturais (não necessariamente aditivos) $\kappa : K \times K \to G$ com $\kappa(a, 0) = 0 = \kappa(0, a)$, $\kappa(a, b) = \kappa(b, a)$ e $\kappa(a, b) + \kappa(a + b, c) = \kappa(a, b + c) + \kappa(b, c)$ para quaisquer $R \in k\text{–}\mathsf{Alg}$ e $a, b, c \in K(R)$; e definimos $B^2(K, G)$ (as "2-cobordas") como a família dos naturais $\kappa : K \times K \to G$ tais que existe natural $\delta : K \to G$ com $\kappa(a, b) = -\delta(a + b) + \delta(a) + \delta(b)$ para quaisquer R e $a, b \in K(R)$. Definimos $H^2_s(K, G)$ como o grupo-quociente $Z^2(K, G)/B^2(K, G)$.

Lema 6.4.10. *Na situação da definição 6.4.8, $\kappa : K \times K \to G$ é um 2-cociclo. Também, se $s' : K \to H$ é outro natural com $g \circ s' = 1_K$ e $s(0) = 0$, associado a κ', então $\kappa - \kappa'$ é uma 2-coborda.*

Demonstração. Use $f(\kappa(a, b) + \kappa(a + b, c)) = -s(a + b) + s(a) + s(b) - s(a + b + c) + s(a + b) + s(c) = -s(a + b + c) + s(a) + s(b) + s(c)$, etc. Também, vale $g \circ (s - s') = 0$, logo $s - s' = f \circ \delta$ para único δ, então $f(\kappa(a, b) - \kappa'(a, b)) = f(-\delta(a + b) + \delta(a) + \delta(b))$. $\square$

Observação 6.4.11. Se $0 \to G \xrightarrow{f'} H' \xrightarrow{g'} K \to 0$ é uma extensão equivalente, isto é, se há isomorfismo $\phi : H \to H'$ com $f' = \phi \circ f$ e $g' \circ \phi = g$, temos $g' \circ (\phi \circ s) = 1_K$ e $(\phi \circ s)(0) = 0$, e obtemos o mesmo 2-cociclo.

Então, temos mapa de $\mathrm{Ext}^1(K, G)_{sec}$ (extensões admitindo seções s) a $H^2_s(K, G)$.

Lema 6.4.12. *Vale que $\mathrm{Ext}^1(K, G)_{sec} \subseteq \mathrm{Ext}^1(K, G)$ é subgrupo, e $\mathrm{Ext}^1(K, G)_{sec} \to H^2_s(K, G)$ é aditivo.*

Demonstração. Dada outra extensão $0 \to G \xrightarrow{f'} H' \xrightarrow{g'} K \to 0$, a soma é assim: primeiro temos $0 \to G \oplus G \to H \oplus H' \to K \oplus K \to 0$, tomamos produto fibrado com $K \to K \oplus K$, (dando $0 \to G \oplus G \to X \to K \to 0$ onde $X(R) \coloneqq \{(a,b) \in (H \oplus H')(R) \mid ga = g'b\}$) e depois soma amalgamada com $G \oplus G \xrightarrow{(a,b)\mapsto a+b} G$, dando $0 \to G \to Y \to K \to 0$ onde Y é conúcleo de $G \xrightarrow{a\mapsto(a,-a)} G \oplus G \xrightarrow{(f,f')} X$. O mapa $H \oplus H' \to K \oplus K$ admite seção $s \oplus s'$, e $X \to K$ admite seção $s'' : K \to X$, $s''k \coloneqq (sk, s'k)$, e $Y \to K$ admite seção $K \xrightarrow{s''} X \xrightarrow{\pi} Y$. (Calcular opostas de extensões: similar). Então, $-\pi(s''(k+k'))+\pi(s''k)+\pi(s''k') = \pi((f\circ\kappa)(k,k'),(f'\circ\kappa')(k,k'))$; usando $\pi(0, f'\circ a) = \pi(f\circ a, 0)$, obtemos o 2-cociclo $\kappa + \kappa'$. □

Observação 6.4.13. Pode-se mostrar que $H^2_s(\_,\_)$ é functor e que o mapa acima é natural.

Lema 6.4.14. *O mapa* $\mathrm{Ext}^1(K,G)_{sec} \to H^2_s(K,G)$ *é isomorfismo.*

Demonstração. Dado 2-cociclo $\kappa : K \times K \to G$, definimos o functor $H \coloneqq K \times G$, com operação $(a,b)+(a',b') \coloneqq (a+a', b+b'+\kappa(a,a'))$. Então, é operação comutativa, $(a, b)+(0,0) = (a, b+0) = (a,b)$, e $(a,b)+(-a,-b-\kappa(a,-a)) = (0,0)$, e associatividade: $((a,b)+(a',b'))+(a'',b'') = (a+a'+a'', b+b'+\kappa(a,a')+b''+\kappa(a+a',a''))$, que é $(a+a'+a'', b+\kappa(a,a'+a'')+b'+b''+\kappa(a',a''))$. Como define operação natural e H também é representável, temos H esquema-grupo afim abeliano. Temos $0 \to G \xrightarrow{f} H \xrightarrow{g} K \to 0$ com $f(b) \coloneqq (0,b)$ e $g(a,b) \coloneqq a$, seção $s(a) \coloneqq (a,0)$, e $s(a)+s(a') = (a+a', \kappa(a,a'))$, e $-s(a+a') = (-a-a', -\kappa(a+a', -a-a'))$, logo $-s(a+a')+s(a)+s(a') = (0, \kappa(a, a')) = (f\circ\kappa)(a,a')$. Então temos sobrejetividade.

Se uma extensão corresponde a κ trivial, temos então $-s(a+b)+s(a)+s(b) = 0$, logo $s : G \to H$ é homomorfismo de grupos, e a extensão cinde. □

Lema 6.4.15. $H^2_s(W_1, W_1)$ *admite* $k[F]$*-ação direita (dada por* $X \mapsto H^2_s(\Phi X, 1)$*), e assim é* $k[F]$*-módulo gerado pelo 2-cociclo* $w : W_1 \times W_1 \to W_1$, $w(x,y) \coloneqq \frac{1}{p}\cdot((x+y)^p - x^p - y^p)$ *(isto é,* $\sum_{i=1}^{p-1} i^{-1}\cdot\binom{p-1}{i-1}\cdot x^{p-i}\cdot y^i$*) [que é o cociclo de* $0 \to W_1 \to W_2 \to W_1 \to 0$*] se a característica é* $p > 0$*.*

Demonstração. (De Demazure e Gabriel (1970) II§3n4) Cada 2-cociclo $W_1 \times W_1 \to W_1$ corresponde a elemento de $f(X,Y) \in W_1(k[X,Y])$, satisfazendo: $f(X,0) = 0 = f(0,Y)$, $f(X,Y) = f(Y,X)$, e a condição $(*)$ $f(X,Y)+f(X+Y,Z) = f(X,Y+Z)+f(Y,Z)$. Cada componente homogênea $P \coloneqq f_n$ satisfaz as duas últimas condições. Escreva $P \coloneqq \sum_{i=0}^n a_i \cdot X^{n-i}\cdot Y^i$. No caso $n = 0$, temos $P = a_0$, que é uma 2-coborda; no caso $n = 1$, temos $P = a_0\cdot(X+Y)$, onde $(*)$ é $a_0\cdot(2\cdot X+\cdots) = a_0\cdot(X+\cdots)$, logo $a_0 = 0$. Supor logo $n \geq 2$.

Denotemos as derivadas ∂_0 e ∂_1. De $(*)$, $\partial_0 P(0,Y)+\partial_0 P(Y,Z) = \partial_0 P(0, Y+Z)$, logo $\partial_0 P(Y,Z) = \sum_{i=0}^n (n-i)\cdot a_i\cdot 0^{n-i-1}\cdot((Y+Z)^i - Y^i) = a_{n-1}\cdot((Y+Z)^{n-1} - Y^{n-1})$. Similarmente, $\partial_1 P(X,Y) = a_1\cdot((X+Y)^{n-1} - Y^{n-1})$. Então, $n\cdot P = X\cdot\partial_0 P + Y\cdot\partial_1 P =$

$X \cdot a_{n-1} \cdot ((X+Y)^{n-1} - X^{n-1}) + Y \cdot a_1 \cdot ((X+Y)^{n-1} - Y^{n-1}) = a_1 \cdot ((X+Y)^n - X^n - Y^n) + (a_{n-1} - a_1) \cdot (X \cdot (X+Y)^{n-1} - X^n)$. E $a_1 = a_{n-1}$ porque P é simétrico. Logo, $n \cdot P = a_1 \cdot ((X+Y)^n - X^n - Y^n)$. Vemos os casos:

- Quando $n \geq 2$ não é múltiplo da característica, vale que P é múltiplo da 2-coborda $(X+Y)^n - X^n - Y^n$.
- Quando $a_1 \neq 0 \in k$ e $n \geq 2$ é múltiplo da característica, vale que $(X+Y)^n - X^n - Y^n = 0$, o que só é possível quando n é potência p^r; logo $\partial_1 P(X,Y) = a_1 \cdot ((X+Y)^{p^r-1} - Y^{p^r-1})$; se $r > 1$, tem o termo $\pm a_1 \cdot \binom{p^r-1}{p-1} \cdot X^{p^r-p} \cdot Y^{p-1}$, mas derivadas em característica p não podem ter termos Y^{p-1}, logo $a_1 \cdot \binom{p^r-1}{p-1} = 0 = a_1 \cdot \frac{(p^r-1)\cdots(p^r-p+1)}{(p-1)\cdots 1}$, então $a_1 = 0$, contradição; então, $r = 1$, e $n = p$; logo $P(X,Y)$ tem a mesma Y-derivada que $a_1 \cdot w(X,Y)$, então $P(X,Y) - a_1 \cdot w(X,Y)$ não tem Y, e por simetria não tem X, logo é constante c, que é uma 2-coborda.
- Quando $a_1 = 0 \in k$ e $n \geq 2$ é múltiplo da característica, por simetria $a_{n-1} = 0$, logo $P(X,Y)$ tem as duas derivadas nulas, logo necessariamente $P = R(X^p, Y^p)$ para algum R, de grau inferior, logo P é a ação $R * F$.

Concluímos que todo f é soma duma 2-coborda com uma combinação linear de termos $w, w*F, \ldots$. Logo, $H^2_s(W_1, W_1)$ é gerado como grupo abeliano pelos múltiplos escalares de $w, w*F, \ldots$, como desejado. □

Lema 6.4.16. *Se $\iota : G \to W_1$ é mônico, $H^2_s(\iota, 1) : H^2_s(W_1, W_1) \to H^2_s(G, W_1)$ é sobrejetivo.*

Demonstração. Seja $k[X]/J$ a álgebra de Hopf de G. O caso $J = 0$ é trivial; supor $J \neq 0$. Existe $0 \neq P \in k[X]$ dalgum grau n tal que $J = k[X] \cdot P$. Se $\kappa : G \times G \to W_1$ é um 2-cociclo, correspondente a $[f] \in k[X,Y]/\langle P(X), P(Y)\rangle$, podemos supor que $\deg_X f, \deg_Y f < n$, logo $f \in (k \cdot X^0 + \cdots + k \cdot X^{n-1}) \cdot (k \cdot Y^0 + \cdots + k \cdot Y^{n-1})$; vale $f(X,0) = 0 = f(0,Y)$, $f(X,Y) \equiv f(Y,X) \pmod{\langle P(X), P(Y)\rangle}$ e $f(X,Y) + f(X+Y, Z) \equiv f(X, Y+Z) + f(Y,Z) \pmod{\langle P(X), P(Y), P(Z)\rangle}$; de fato valerão igualdades por causa dos graus, logo f corresponde a 2-cociclo $W_1 \times W_1 \to W_1$. □

Lema 6.4.17. *Se G é esquema-grupo afim abeliano,* $\mathrm{Ext}^1(G, W_1)_{sec} = \mathrm{Ext}^1(G, W_1)$.

Demonstração. Seja extensão $0 \to W_1 \xrightarrow{f} H \xrightarrow{g} G \to 0$ de esquemas-grupos afins abelianos. Há natural $\sigma : H \times_G H \to \mathrm{nuc}(H \to G) \cong W_1$ dado por $(a,b) \mapsto f^{-1}(a-b)$; seja seu correspondente $\sigma' \in k\text{–}\mathsf{Alg}(k[X], A_H \otimes_{A_G} A_H)$.

Sendo g epimorfismo, corresponde a injeção $g' : A_G \to A_H$ de álgebras de Hopf, que é fielmente plana (teorema 4.5.13), logo $0 \to A_G \to A_H \xrightarrow{\delta} A_H \otimes_{A_G} A_H \xrightarrow{\delta'} A_H \otimes_{A_G} A_H \otimes_{A_G} A_H$, onde $\delta x := x \otimes 1 - 1 \otimes x$ e $\delta'(x \otimes y) := x \otimes y \otimes 1 - x \otimes 1 \otimes y + 1 \otimes x \otimes y$, é

sequência exata de A_G-módulos: a exatidão em A_H é do lema 4.5.6, e a em $A_H \otimes_{A_G} A_H$ tem prova similar.

Como $(a,b,c) \in H \times_G H \times_G H \mapsto \sigma(a,b)$ corresponde a $k[X] \xrightarrow{\sigma'} A_H \otimes_{A_G} A_H \xrightarrow{u_2} A_H \otimes_{A_G} A_H \otimes_{A_G} A_H$, onde $u_2(x \otimes y) \coloneqq x \otimes y \otimes 1$, a propriedade $\sigma(a,b)+\sigma(b,c) = \sigma(a,c)$ implica que $\langle u_2 \circ \sigma', u_0 \circ \sigma' \rangle \circ \Delta = u_1 \circ \sigma'$; avaliando em X, usando $\delta' = u_0 - u_1 + u_2$, então $\delta'(\sigma' X) = 0$. Por exatidão, $\sigma' X = \tilde{z} \otimes 1 - 1 \otimes \tilde{z}$ para algum $\tilde{z} \in A_H$.

Temos natural (não necessariamente homomorfismo de grupos) $h : H \to H$ dado por $a \in H(R) = k\text{−}\mathsf{Alg}(A_H, R) \mapsto a - f(X \mapsto a\tilde{z})$, que corresponde à seta $h' \in k\text{−}\mathsf{Alg}(A_H, A_H)$ dada por $\langle 1, A_{\tilde{z}} \circ f' \circ S \rangle \circ \Delta$, onde $A_{\tilde{z}} X \coloneqq \tilde{z}$. Notar que $(a, b) \in H \times_G H$ implica $a - b = f(\sigma(a,b)) = f(X \mapsto \langle a, b \rangle(\sigma' X)) = f(X \mapsto a\tilde{z} - b\tilde{z})$, logo $a - f(X \mapsto a\tilde{z}) = b - f(X \mapsto b\tilde{z})$. Noutras palavras, os dois mapas $H \times_G H \rightrightarrows H \xrightarrow{h} H$ coincidem, isto é, os dois mapas $A_H \xrightarrow{h'} A_H \rightrightarrows A_H \otimes_{A_G} A_H$ coincidem. Pelo lema 4.5.6, a imagem de h' está dentro de $A_G \subseteq A_H$, logo induz seta $\overline{h}' : k\text{−}\mathsf{Alg}(A_H, A_G)$, que corresponde a natural (não necessariamente homomorfismo de grupos) $\overline{h} : G \to H$ tal que $\overline{h} \circ g = h$. Portanto, g admite seção $\overline{h}$ (isto é, $g \circ \overline{h} = 1_G$) porque $h' \circ g' = \langle g', A_{\tilde{z}} \circ f' \circ g' \circ S \rangle \circ \Delta = \langle g', A_{\tilde{z}} \circ \epsilon \circ S \rangle \circ \Delta = \langle g', \epsilon \rangle \circ \Delta = g'$ (continência $A_G \to A_H$), logo $\overline{h}' \circ g' = 1_{A_G}$. □

Assim podemos terminar a prova do lema 6.4.7. Seja mônico $G \to W_1$; então $\mathrm{Ext}^1(G, W_1) = \mathrm{Ext}^1(G, W_1)_{sec} \cong H^2_s(G, W_1)$, por 6.4.17, 6.4.14; e os itens (b) e (c) (para $n = 1$) do lema a ser provado estão em 6.4.16, 6.4.15.

6.4.2 A prova

Lembremos que queremos provar que se $G \to H$ é mônico, então $M(G) \leftarrow M(H)$ é sobrejetivo. Outra vez se usa (Demazure e Gabriel, 1970 V§1).

Lema 6.4.18. *Se $\iota : G \to H$ é mônico na categoria dos esquemas-grupos afins abelianos e cujo conúcleo é subgrupo fechado de W_1, e dado $f : G \to W_n$, existe $g : H \to W_{n+1}$ com $(v : W_n \to W_{n+1}) \circ f = g \circ \iota$.*

Demonstração. Temos sequência exata $E \coloneqq (0 \to G \to H \to K \to 0) \in \mathrm{Ext}^1(K, G)$ onde $K \to W_1$ é mônico. Pelo lema 6.4.7, $\mathrm{Ext}^1(K, W_n)$ é quociente de $\mathrm{Ext}^1(W_1, W_n)$, que é gerado como $k[F]$-módulo direito por um só elemento, que se anula ao aplicar $\mathrm{Ext}^1(1, v : W_n \to W_{n+1})$. Logo, $\mathrm{Ext}^1(1, v \circ f)(E) \in \mathrm{Ext}^1(1, v)(\mathrm{Ext}^1(K, W_n)) = 0$; logo há sequência exata cindível $0 \to W_{n+1} \to X \to K \to 0$ onde X é produto fibrado de $G \to H$ e $G \to W_{n+1}$; logo $g \coloneqq (H \to X \to W_{n+1})$ satisfaz $g \circ \iota = (G \to X \to W_{n+1}) = v \circ f$. □

Lema 6.4.19. *Se $G \neq 0$ está em $\mathcal{C}$, há não nula $G \to W_1$.*

Demonstração. Supõe-se que não. Logo $\forall_{x\in A_G}\Delta x = x\otimes 1 + 1\otimes x \implies x = 0$. Sendo $\beta_\bullet$ base de $\overline{k}$ sobre k, dado $x \in (A_G)_{\overline{k}}$ com $\Delta x = x\otimes 1 + 1\otimes x$, escrevendo $x = \sum_i \beta_i \cdot (x_i \in A_G)$, vale $\sum_i \beta_i \cdot \Delta x_i = \sum_i \beta_i \cdot (x_i \otimes 1 + 1 \otimes x_i)$, logo cada $x_i = 0$, e $x = 0$. Logo, supomos, SPDG, $k = \overline{k}$.

Existe subcoálgebra $C \subseteq A$ de dimensão finita com $C \supsetneq k$ (porque $A \supsetneq k$). Como V é "nilpotente" em C, F é "nilpotente" na álgebra C^*, logo C^* é álgebra local. Seja M o ideal maximal de C^*; logo, $C^*/M \cong k$ porque $k = \overline{k}$. Seja $[f_1]$, $\ldots, [f_n]$ base de M/M^2. Define-se $\Phi : M/M^2 \to k[X]/(X^2)$ por $\Phi[f_i] \coloneqq X$; e linear $\phi : C^* \to k[X]/(X^2)$ por $\phi(1) \coloneqq 1$ e $\phi(g \in M) \coloneqq \Phi[f]$. Então, ϕ é homomorfismo de álgebras. Existem $a, b \in C$ com $\forall_{f\in C^*}\phi f = fa + X\cdot fb$. Como $\phi(\langle f, g\rangle \circ \Delta) = \phi f \cdot \phi g$, vale $\langle f, g\rangle(\Delta a) + X\cdot\langle f, g\rangle(\Delta b) = fa\cdot ga + X\cdot(fa\cdot gb + fb\cdot ga)$; também $\phi\epsilon = 1$, e $\epsilon a + X\cdot\epsilon b = 1$; como $f, g \in C^*$ são arbitrários, $\epsilon a = 1$, $\epsilon b = 0$, $\Delta a = a\otimes a$, $\Delta b = a\otimes b + b\otimes a$; logo, a é quase de grupo, $a^{-1} = Sa$, e $\Delta(a^{-1}\cdot b) = 1\otimes(a^{-1}\cdot b) + (a^{-1}\cdot b)\otimes 1$; então, $a^{-1}\cdot b = 0$, logo X não está na imagem de ϕ; como $\forall_{1\le i\le n}\phi(f_i) = X$, vale $n = 0$, logo $M = M^2 = M^4 = \cdots = 0$, e $\dim C^* = 1$, contradição. □

Observação 6.4.20. Assim, os objetos de $\mathcal{C}$ são "unipotentes".

Lema 6.4.21. *Se G está em $\mathcal{C}$ e é algébrico, existem $n, a, b \in \mathbb{N}$ e sequência exata $0 \to G \to W_n^{\oplus a} \to W_n^{\oplus b}$.*

Demonstração. Provamos inicialmente que existe mônico $G \to W_n^{\oplus a}$. Os subgrupos fechados de G estão em bijeção com os ideais de Hopf de A_G, noetheriana; logo, toda família não vazia de subgrupos fechados tem membro minimal; em particular, pode-se provar por indução forte nos subgrupos fechados de G.

O caso $G = 0$ é trivial. Supor $G \neq 0$. Pelo lema anterior, existe não nulo $f : G \to W_1$. Logo, $\operatorname{nuc} f \subsetneq G$, e por hipótese indutiva existem $0 \to \operatorname{nuc} f \to W_n^{\oplus a}$. Pelo lema 6.4.18, usando $G/\operatorname{nuc} f \subseteq W_1$, cada um dos $\operatorname{nuc} f \to W_n \to W_{n+1}$ estende-se a $G \to W_{n+1}$. Usando também $G \xrightarrow{f} W_1 \xrightarrow{v^n} W_{n+1}$, temos $G \to W_{n+1}^{\oplus(a+1)}$. É mônico, pois se $x \in G(R)$ está no núcleo, em particular $v^n(fx) = 0$, logo $x \in \operatorname{nuc} f(R)$, e usamos que $\operatorname{nuc} f \to W_n^{\oplus a}$ é mônico para concluir $x = 0$.

Então temos sempre mônico $0 \to G \to W_n^{\oplus a}$. Sendo o conúcleo $H \coloneqq W_n^{\oplus a}/G$, assim também há mônico $H \to W_m^{\oplus b}$; usando $W_m \xrightarrow{v^n} W_{m+n}$, pode-se supor $m \ge n$; o núcleo de $W_n^{\oplus a} \twoheadrightarrow H \hookrightarrow W_m^{\oplus b}$ é $G \to W_n^{\oplus a}$. Então, $0 \to G \to W_n^{\oplus a} \xrightarrow{\phi} W_m^{\oplus b}$ é exata; o mapa ϕ satisfaz $V^n \circ \phi = \phi^{(p)^{-n}} \circ V^n = 0$, logo ϕ pode ser fatorado $W_n^{\oplus a} \to W_n^{\oplus a} \xrightarrow{(v^{m-n})^{\oplus a}} W_m^{\oplus a}$, logo há exata $0 \to G \to W_n^{\oplus a} \to W_n^{\oplus b}$. □

Lema 6.4.22. *Se $G \to H$ é mônico em $\mathcal{C}$ e H é algébrico então existe fatoração $G = G_n \to \cdots \to G_0 = H$ em mônicos onde cada quociente G_i/G_{i+1} é isomorfo a subgrupo fechado de W_1.*

Demonstração. Pelo lema 6.4.19, se $H/G \neq 0$, há não nulo $H/G \to W_1$, isto é, não nulo $f : H \to W_1$ anulando-se em G, isto é, $G \subseteq \operatorname{nuc} f \subsetneq H$ e $H/\operatorname{nuc} f \subseteq W_1$. Então: se $H = G$, provado; senão, há $G \subseteq G_1 \subsetneq H$ com $H/G_1 \subseteq W_1$; se $G_1 = G$, provado; senão, há $G \subseteq G_2 \subsetneq G_1$ com $G_1/G_2 \subseteq W_1$; etc. A sequência $G_1 \supsetneq G_2 \supsetneq \cdots$ deve ter membro minimal porque G é algébrico, logo deve ser finita. □

Lema 6.4.23. *Se $G \to H$ é mônico em $\mathcal{C}$, então $M(G) \leftarrow M(H)$ é sobrejetivo. Isto é, M é exato direito também.*

Demonstração. Seja $A_G = A_H/J$. Como A_H é união direcionada de subálgebras de Hopf finitamente geradas A_i, também A_G é união direcionada das $A_i/(J \cap A_i)$, e vale $H \cong \lim_i H_i$ e $G \cong \lim_i G_i$, e $MH \cong \operatorname{co\lim}_i H_i$ e $MG \cong \operatorname{co\lim}_i G_i$. Se provarmos cada $M(G_i) \leftarrow M(H_i)$ sobrejetivo, o mapa $MG \leftarrow MH$ será a união, logo será sobrejetivo também.

Logo, SPDG, H é algébrico. Pelo lema anterior, há mônicos $G = G_n \to \cdots \to G_0 = H$ onde cada G_i/G_{i+1} é isomorfo a subgrupo fechado de W_1. Dado elemento de $M(G)$, na forma $f : G \to W_m$, o lema 6.4.18 repetido dá $h : G \to W_{n+m}$ com $v^n \circ f = h \circ \iota$, logo $M\iota[h] = [f]$. □

Lema 6.4.24. *$M : \mathcal{C}^\circ \to \mathcal{D}$ é pleno fiel.*

Demonstração. Dados G, H em $\mathcal{C}$, queremos mostrar $\hom(G, H) \to \hom(MH, MG)$ bijetivo; SPDG, H é algébrico. Logo há sequência exata $0 \to H \to W_n^{\oplus a} \to W_n^{\oplus b}$. Já provamos que M é exato, logo $0 \leftarrow MH \leftarrow MW_n^{\oplus a} \leftarrow MW_n^{\oplus b}$ é exata. Lembrar $MW_n^{\oplus a} \cong (MW_n)^{\oplus a} \cong (\frac{E}{E \cdot V^n})^{\oplus a}$. Então:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \hom(G,H) & \longrightarrow & \hom(G, W_n^{\oplus a}) & \longrightarrow & \hom(G, W_n^{\oplus b}) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \hom(MH, MG) & \longrightarrow & \hom((\frac{E}{E \cdot V^n})^{\oplus a}, MG) & \longrightarrow & \hom((\frac{E}{E \cdot V^n})^{\oplus b}, MG) \end{array}$$

diagrama comutativo com duas linhas exatas. Vale $\hom(\frac{E}{E \cdot V^n}, MG) \cong \{[f : G \to W_{(\cdots)}] \in MG \mid [v^n \circ f : G \to W_{(\cdots)}] = 0\} \cong \hom(G, W_n)$. Então o mapas verticais do meio e da direita são isomorfismos; por lema de homologia, o mapa vertical da esquerda também é isomorfismo. □

Lema 6.4.25. *M é essencialmente sobrejetivo.*

Demonstração. Seja primeiro X em $\mathcal{D}$ finitamente gerado. Então há N com $V^N(X) = 0$, logo X é $\frac{E}{E \cdot V^N}$-módulo; como $\frac{E}{E \cdot V^N}$ é noetheriano (lema 6.3.4), existe sequência exata $(\frac{E}{E \cdot V^N})^{\oplus b} \xrightarrow{\phi} (\frac{E}{E \cdot V^N})^{\oplus a} \to X \to 0$. Como $M(W_N^{\oplus a}) \cong (\frac{E}{E \cdot V^N})^{\oplus a}$ e vimos M pleno fiel, ϕ é da forma $M(W_N^{\oplus a} \xrightarrow{\psi} W_N^{\oplus b})$; logo $0 \to \operatorname{nuc} \psi \to W_N^{\oplus a} \to W_N^{\oplus b}$ é exata, e como

M é exato, vale $(\frac{E}{E\cdot V^N})^{\oplus b} \to (\frac{E}{E\cdot V^N})^{\oplus a} \to M(\operatorname{nuc}\psi) \to 0$ exato também, o que implica $X \cong M(\operatorname{nuc}\psi)$.

No caso geral, X é união direcionada de X_i finitamente gerados, e cada $X_i \cong M(G_i)$; os injetivos $X_i \to X_j$ correspondem a épicos $G_i \leftarrow G_j$, e mônicos $A_i \to A_j$; sendo A a união direcionada das A_i, associada a G, temos então $MG \cong \operatorname{co\lim}_i MG_i \cong \operatorname{co\lim}_i MX_i \cong X$. □

Exemplo 6.4.26. Como W_n^m é núcleo de $F^m : W_n \to W_n$, MW_n^m é conúcleo de $MF^m \in \operatorname{End}(MW_n) \cong \operatorname{End}(\frac{E}{E\cdot V^n})$; temos $MF^m[\Phi X : W_n \to W_n] \coloneqq [\Phi X \circ F^m] = [\Phi(X \cdot F^m)]$; logo, MF^m corresponde ao endomorfismo $X \mapsto X \cdot F^m$ em $\operatorname{End}(\frac{E}{E\cdot V^n})$; então $MW_n^m \cong \frac{E}{E\cdot V^n + E\cdot F^m}$.

Exemplo 6.4.27. Dado E-módulo simples X em $\mathcal{D}$, vale $0 \neq \operatorname{nuc}(V\cdot\_)$, logo $\operatorname{nuc}(V\cdot\_) = X$, isto é, $V \cdot X = 0$. Então, X é um $\frac{E}{E\cdot V}$-módulo, onde $\frac{E}{E\cdot V} = \bigoplus_{i\geq 0} \frac{W(k)}{\langle p\rangle}\cdot F^i \cong k[F]$, cujos ideais esquerdos, similarmente ao anel polinomial, são $\langle P(F)\rangle$, para polinômios P; logo, $X \cong k[F]/\langle P(F)\rangle$, onde P é irredutível; isto é, X é conúcleo de $\_\cdot P(F) \in \operatorname{End}(k[F]) \cong \operatorname{End}(MW_1)$, logo X é MH onde H é núcleo de $P(F)\cdot\_ \in \operatorname{End}(W_1)$, isto é, $H(R) \coloneqq \{x \in R \mid P(F)(x) = 0\}$, onde $Fx \coloneqq x^p$. Notar $A_H = k[X]/\langle P(F)(X)\rangle$, que tem dimensão finita.

Teorema 6.4.28. *O functor de Dieudonné M é antiequivalência da categoria dos esquemas-grupos afins abelianos G sobre um corpo perfeito de k característica $p > 0$ onde A_G satisfaz $\forall_{x\in\operatorname{nuc}\epsilon\subseteq A_G}\exists_N V^N(x) = 0 \in A_G^{(p)^N}$, à categoria dos E-módulos X satisfazendo $\forall_{x\in X}\exists_N V^N\cdot x = 0$. Também, G é algébrico se e só se MG é E-finitamente gerado; G é finito se e só se MG é de k-dimensão finita, e neste caso $\log_p \dim A_G$ é a k-dimensão de MG.*

Demonstração. Os lemas acimas provaram M ser antiequivalência. Agora, $G \in \mathcal{C}$ é algébrico sse há mônico $G \to W_n^{\oplus a}$, sse há épico $MW_n^{\oplus a} \cong (\frac{E}{E\cdot V^n})^{\oplus a} \to MG$, sse MG é E-finitamente gerado (e assim havendo n com $V^n(MG) = 0$).

Se G é finito, é de "comprimento finito", isto é, sequências de epimorfismos $G \to \cdots \to 0$ que não são isomorfismos (logo necessariamente reduzindo as dimensões) têm comprimento limitado; logo MG é de E-comprimento finito também; é dado por repetidas extensões, iniciando em E-simples, que pelo exemplo acima são da forma $k[F]/\langle P(F)\rangle$, P irredutível, que tem k-dimensão finita.

Na outra direção, se MG tem k-dimensão finita, é dado por repetidas extensões, iniciando em E-simples; logo G é dado por repetidas extensões, iniciando nos H com $H(R) \coloneqq \{x \in R \mid P(F)(x) = 0\}$, P polinômio irredutível, que é finito; logo G é finito também.

Vale que $\dim k[F]/\langle P(F)\rangle$ é o grau d de P, enquanto $\dim A_H = \dim k[X]/\langle P(F)(X)\rangle$ é p^d. Então neste caso vale $\log_p \dim A_G = \dim MG$. Segue de que, em

cada sequência exata $0 \to G \to H \to K \to 0$, vale $\dim A_H = \dim A_G \cdot \dim A_K$ e $\dim MH = \dim MG + \dim MK$. □

Corolário 6.4.29. *Há antiequivalência entre as categorias dos esquemas-grupos afins abelianos finitos (sobre corpo perfeito de característica $p > 0$) cujos duais de Cartier têm álgebras de Hopf conexas (isto é, locais) e a categoria dos E-módulos que têm k-dimensões finitas em que V age nilpotentemente.*

Demonstração. No caso G finito, pelo lema 5.1.9, A^* é conexa sse F_{A^*} é "nilpotente", isto é, sse V_A é "nilpotente", sse G está no domínio da antiequivalência de Dieudonné; logo segue do teorema anterior. □

6.4.3 Relação com duais

Definição 6.4.30. Seja k (de novo) corpo perfeito de característica $p > 0$. Lembrando que $W(k)$ é um domínio (lema 6.1.12), define-se $W_\infty(k) \coloneqq \frac{\operatorname{Frac} W(k)}{W(k)}$. Para cada $W(k)$-módulo esquerdo X, define-se $D(X) \coloneqq W(k)\text{−}\mathsf{Mod}(X, W_\infty(k))$. Se adicionalmente, X é E-módulo esquerdo, define-se estrutura de E-módulo em $D(X)$ por: $F \cdot (f \in D(M)) \coloneqq ((\_)^\sigma \circ f \circ V)$, $V \cdot f \coloneqq ((\_)^{\sigma^{-1}} \circ f \circ F)$. (Notar que, por exemplo, $F \cdot f$ é $W(k)$-linear porque $(F \cdot f)(\xi \cdot x) = (f(V \cdot \xi \cdot x))^\sigma = (f(\xi^{\sigma^{-1}} \cdot V \cdot x))^\sigma = \xi \cdot (f(V \cdot x))^\sigma$. Também, $V \cdot (F \cdot f) = (\_)^{\sigma^{-1}} \circ (\_)^\sigma \circ f \circ V \circ F = p \cdot f$, $V \cdot (\xi \cdot f) = \xi^{\sigma^{-1}} \cdot (V \cdot f)$, etc).

Lema 6.4.31. $D_n(X) \coloneqq \{f \in D(X) \mid F^n \cdot f = V^n \cdot f = 0\} \cong E\text{−}\mathsf{Mod}(X, \frac{E}{E \cdot F^n + E \cdot V^n})$.

Demonstração. Lembrar que os elementos de $\frac{E}{E \cdot F^n + E \cdot V^n}$ são da forma $\sum_{i=1}^{n-1} \xi_i \cdot F^i + \xi_0 + \sum_{i=1}^{n-1} \xi_{-i} \cdot V^i$, onde $\xi_{\pm i} \in W_{n-i}(k)$. Assim, um E-linear $f : X \to \frac{E}{E \cdot F^n + E \cdot V^n}$ é o mesmo que $W(k)$-lineares $f_i : X \to W_{n-|i|}(k)$, $-n < i < n$, tais que $\sum_i X_i \cdot (f_i \circ X_j) = X_j \cdot \sum_i X_i \cdot f_i$ (que é $\sum_i p^{(\cdots)} \cdot X_{i+j} \cdot f_i$), para cada j. A condição equivale a: $p^{|j|} \cdot f_{-j} = f_0 \circ X_j$ para cada j. Então, os elementos de $E\text{−}\mathsf{Mod}(X, \frac{E}{E \cdot F^n + E \cdot V^n})$ são determinados pelos $W(k)$-lineares $f_0 : X \to W_n(k)$ com cada $f_0(X_j x) \in W_n(k)$, $x \in X$ e $|j| \leq n$, iniciando com $\geq |j|$ zeros. De fato, basta a condição $f_0 \circ F^n = 0 = f_0 \circ V^n$: pois assim, $p^{n-j} \cdot f_0(F^j x) = f_0(p^{n-j} \cdot F^j x) = f_0(F^n V^{n-j} x) = 0$, logo $f_0(F^j x)$ inicia com $n - j$ zeros, e similarmente também $f_0(V^j x)$.

Os $f \in D_n(X)$ satisfazem $p^n \cdot f = 0$, isto é, toda imagem $f(x) \in \frac{\operatorname{Frac} W(k)}{W(k)}$ é da forma $[y/p^n]$ onde $[y] \in W(k)/\langle p^n \rangle \cong W_n(k)$. Assim, $D_n(X) \cong \{f \in W(k)\text{−}\mathsf{Mod}(X, W_n(k)) \mid f \circ F^n = 0 = f \circ V^n\} \cong E\text{−}\mathsf{Mod}(X, \frac{E}{E \cdot F^n + E \cdot V^n})$. □

A antiequivalência de Dieudonné restringe-se a antiequivalência entre a categoria dos esquemas-grupos abelianos finitos de tipo local-local (isto é, em que F e V são "nilpotentes") e a categoria dos E-módulos esquerdos de k-dimensões finitas em que F e V agem nilpotentemente. Se X é um desses E-módulos, então F e V também agem nilpotentemente em $D(X)$.

Lema 6.4.32. *Se G é um esquema-grupo abeliano finito de tipo local-local, então $M(G^*) \cong D(M(G))$ naturalmente.*

Demonstração. Como G é de tipo local-local, existe n tal que F^n e V^n se anulam em G^*, logo todo $G \to W_{m+n}$ se fatora $G \to W_n^n \to W_{m+n}$. Então, $M(G^*) \cong \operatorname{co\lim}_n \mathsf{Ab}^{k-\mathsf{Alg}}(G^*, W_n^n) \cong \operatorname{co\lim}_n \mathsf{Ab}^{k-\mathsf{Alg}}((W_n^n)^*, G) \cong \operatorname{co\lim}_n \mathsf{Ab}^{k-\mathsf{Alg}}(W_n^n, G)$, usando que dualidade de Cartier é antiequivalência e o teorema 6.2.12. E $\mathsf{Ab}^{k-\mathsf{Alg}}(W_n^n, G) \cong E{-}\mathsf{Mod}(MG, MW_n^n) \cong E{-}\mathsf{Mod}(MG, \frac{E}{E\cdot F^n + E\cdot V^n})$ pelo exemplo 6.4.26. Logo, pelo lema anterior, $M(G^*) \cong \operatorname{co\lim}_n D_n(MG) \cong D(MG)$, porque há n em que F^n e V^n se anulam em MG. □

Corolário 6.4.33. *O functor de Dieudonné estende-se a antiequivalência M' (notação temporária) entre a categoria dos esquemas-grupos afins abelianos de ordens finitas $\in \{p^0, p^1, \ldots\}$ sobre o corpo perfeito k de característica $p > 0$ e a categoria dos E-módulos esquerdos de $W(k)$-comprimentos finitos. Vale: (a) $M'(G^*) \cong D(M'G)$ naturalmente; (b) a k-dimensão de $M'G$ é $\log_p|G|$.*

Demonstração. Se G tem ordem $\in \{p^0, p^1, \ldots\}$, decompõe-se functorial e unicamente (a menos de únicos isomorfismos) nas quatro partes $G \cong G_{rr} \oplus G_{rl} \oplus G_{lr} \oplus G_{ll}$, e a ordem de G é o produto das ordens das partes. A parte G_{rr} tem álgebra de Hopf A reduzida (isto é, separável) com A^* também reduzida; em particular, $A \otimes k_s \cong k_s^{\dim_k A}$, logo é a álgebra de Hopf k_s^Z para certo grupo finito abeliano Z (fato 4.2.4), e $(k_s^Z)^* \cong k_s[Z]$; para cada $x \in Z$, vale $(e_x - e_1)^p = e_{x^p} - e_1$, e como $k_s[Z]$ é reduzida, $x^p = 1 \implies x = 1$. Então, $|Z|$ não pode ter fator primo p; como $|G_{rr}| = |Z|$ deve ser potência de p, vale $Z = 0$, e $G_{rr} \cong 0$.

As partes G_{rl} e G_{ll} já estão no domínio da antiequivalência de Dieudonné de antes. Logo, definimos $M'G := MG_{rl} \oplus D(M(G_{lr}^*)) \oplus MG_{ll}$.

Se X tem $W(k)$-comprimento finito, por teorema de classificação de módulos sobre domínio de ideais principais, vale que $X \cong \bigoplus_i W(k)/\langle p^{e_i}\rangle \cong \bigoplus_i W_{e_i}(k)$ (só $W(k)$-linear) para certos expoentes e_i, e $DX \cong \bigoplus_i W(k){-}\mathsf{Mod}(W_{e_i}(k), \frac{\operatorname{Frac} W(k)}{W(k)}) \cong \bigoplus_i W(k){-}\mathsf{Mod}(W_{e_i}(k), \frac{W(k)}{\langle p^{e_i}\rangle}) \cong \bigoplus_i W_{e_i}(k)$. Logo, DX tem o mesmo $W(k)$-comprimento que X (e também a mesma k-dimensão).

Adicionalmente, se X é E-módulo com $W(k)$-comprimento finito, $D(DX)$ também tem o mesmo comprimento, logo o mapa E-linear injetivo canônico $X \to D(DX)$ tem que ser isomorfismo. Então, de $G^* \cong G_{lr}^* \oplus G_{rl}^* \oplus G_{ll}^*$, pelo lema anterior vale $MG_{ll}^* \cong D(MG_{ll})$, logo $M'G^* \cong MG_{lr}^* \oplus D(M(G_{rl}^{**})) \oplus M(G_{ll}^*) \cong D\big(M(G_{rl}) \oplus D(M(G_{lr}^*)) \oplus MG_{ll}\big) \cong D(M'G)$.

Também, $\dim_k M'G = \log_p|G_{rl}| + \log_p|G_{ll}| + \log_p|G_{lr}^*| = \log_p|G|$.

Resta provar M' antiequivalência. Se $X \in E{-}\mathsf{Mod}$ tem $W(k)$-comprimento finito, pelo teorema de Hans Fitting em álgebra linear existe n com $X \cong \operatorname{nuc}(F^n) \oplus \operatorname{im}(F^n)$ onde também F é bijetivo em $\operatorname{im}(F^n)$, e existe m com $X' \cong (X' \cap \operatorname{nuc}(V^m)) \oplus$

$(X' \cap \mathrm{im}(V^m))$ onde V também é bijetivo em $X' \cap \mathrm{im}(V^m)$, para cada $X' = \mathrm{nuc}(F^n)$, $\mathrm{im}(F^n)$. As parcelas $(\cdots) \cap \mathrm{nuc}(V^m)$ já estão na imagem essencial do functor M de antes. Também, V^n anula-se em $D(\mathrm{nuc}(F^n) \cap \mathrm{im}(V^m))$, logo este módulo é da forma MH, logo $\mathrm{nuc}(F^n) \cap \mathrm{im}(V^m) \cong D(MH) \cong M'H^*$. E a última parcela $\mathrm{im}(F^n) \cap \mathrm{im}(V^m)$ tem $p = F \circ V$ bijetivo, logo a decomposição do $W(k)$-módulo como $\bigoplus_i W_{e'_i}(k)$ mostra que $\mathrm{im}(F^n) \cap \mathrm{im}(V^m)$ é nulo. Então, $X \cong M'H$ para algum H.

Similarmente, para cada E-linear $f : X \to Y$ entre módulos de $W(k)$-comprimento finito, existem n e m tais que X e Y se decompõem em $(\mathrm{nuc}(F^m) \cap \mathrm{nuc}(V^m)) \oplus \cdots$, e f também se decompõe. Como M é functor pleno fiel, e $G_{lr} \mapsto D(M(G_{lr}^*))$ também é pleno fiel (porque $(\_) \cong D(D\_)$), conclui-se que M' é pleno fiel. $\square$

Capítulo 7

Os esquemas-grupos p-divisíveis

Seja k corpo perfeito de característica $p > 0$.

7.1 O básico

Definição 7.1.1. Um esquema-grupo formal abeliano G é dito "p-divisível" de "altura h" quando $G_n \coloneqq \mathrm{nuc}(p^n : G \to G)$ satisfazem: $G = \bigcup_n G_n$; G_1 tem ordem p^h; e $p : G \to G$ é epimorfismo.

Exemplo 7.1.2. Seja $G(R) \coloneqq \{r \in R^\times \mid \exists_n r^{p^n} = 1\}$, no produto. Então, $G = \bigcup_n \underline{\mu}_{p^n}$, com $\mathrm{nuc}(p^n : G \to G) = \underline{\mu}_{p^n}$; como $\underline{\mu}_p$ tem álgebra $k[X]/(X^p - 1)$, tem ordem p^1; cada $p : \underline{\mu}_{p^{n+1}} \to \underline{\mu}_{p^n}$ é épico (porque $k[X]/(X^{p^n} - 1) \to k[X]/(X^{p^{n+1}} - 1)$, $X \mapsto X^p$, é mônico). Portanto, G é p-divisível de altura 1.

Lema 7.1.3. *Se G é esquema-grupo formal p-divisível de altura h, vale: cada $\forall_{i,j\geq 0} 0 \to G_i \hookrightarrow G_{i+j} \xrightarrow{p^i} G_j \to 0$ é exata; cada G_n tem ordem $p^{n\cdot h}$.*

Demonstração. Como cada $G \xrightarrow{p^i} G$ é epimorfismo, há sequência exata $0 \to G_i \to G \xrightarrow{p^i} G \to 0$ de esquemas-grupos formais abelianos (que, lembrando, formam categoria abeliana, cujos limites finitos são os mesmos que de functores). Aplicando $\mathrm{Ext}^1(G_j \to G, 1)$, obtemos sequência exata $0 \to G_i \to H \to G_j \to 0$ onde $H(R) = \{(a, b) \in G(R) \times G_j(R) \mid p^i \cdot a = b\} \cong \{a \in G(R) \mid p^j \cdot p^i \cdot a = 0\} = G_{i+j}(R)$. Então, $0 \to G_i \to G_{i+j} \xrightarrow{p^i} G_j \to 0$ é exata. Como $G_0 = 0$ tem ordem $p^{0\cdot h}$, G_1 tem ordem $p^{1\cdot h}$, e como cada $0 \to G_1 \to G_{1+j} \to G_j \to 0$ é exata, vale $|G_{1+j}| = |G_j| \cdot p^h$, logo segue por indução. □

Exemplo 7.1.4. Se G é p-divisível, cada $G_{n+1} \xrightarrow{p} G_n$ é épico, logo seu dual $G_n^* \xrightarrow{p^*} G_{n+1}^*$ é mônico; seja $G^{(*)} \coloneqq \mathrm{co}\lim_n G_n^*$. Como $0 \to G_m \xrightarrow{i^n} G_{m+n} \xrightarrow{p^m} G_n \to 0$ é exata, $0 \to G_n^* \xrightarrow{(p^m)^*} G_{m+n}^* \xrightarrow{(i^n)^*} G_m^* \to 0$ é exata; em particular, $\mathrm{nuc}((i^n)^* : G_{m+n}^* \to G_m^*) = \mathrm{nuc}(p^n = (p^n)^* \circ (i^n)^* : G_{m+n}^* \to G_{m+n}^*) \cong G_n^*$, para cada m; logo, $\mathrm{nuc}(p^n : G^{(*)} \to G^{(*)}) \cong G_n^*$. O

mapa $p : G^{(*)} \to G^{(*)}$ é épico porque cada $i^* : G^*_{m+1} \to G^*_m$ é épico. Portanto, $G^{(*)}$ é p-divisível de mesma altura que G.

Definição 7.1.5. Dado G esquema-grupo formal abeliano p-divisível de altura h, define-se MG como o E-módulo esquerdo limite de $MG_0 \leftarrow MG_1 \leftarrow \cdots$ (onde cada MG_n tem ordem $\in \{p^0, p^1, \ldots\}$ pelo lema 7.1.3).

Corolário 7.1.6. *O functor de Dieudonné estende-se a antiequivalência da categoria dos esquemas-grupos formais abelianos p-divisíveis à categoria dos E-módulos esquerdos que são $W(k)$-livres finitamente gerados.*

Demonstração. Como $W(k)$ é domínio de ideais principais, por certo teorema de classificação há $W(k)$-isomorfismos $MG_n \cong \bigoplus_{l\in\mathbb{N}} W_{e(n,l)}(k)$, em ordem decrescente dos índices $e(n,l)$. Como MG_n tem k-dimensão igual à ordem $|G_n| = n \cdot h$, vale $\sum_l e(n, l) = n \cdot h$. Como $0 \to G_n \to G_{n+1} \xrightarrow{p^n} G_{n+1}$ é exata, $0 \leftarrow MG_n \leftarrow MG_{n+1} \xleftarrow{p^n} MG_{n+1}$ é exata, logo $MG_n \cong \frac{MG_{n+1}}{p^n \cdot MG_{n+1}}$; vale $p^n \cdot \bigoplus_l W_{e(n+1,l)}(k) = \bigoplus_l V^n W_{e(n+1,l)}(k)$, logo $e(n,l) = \min(n, e(n+1,l))$.

Prova-se por indução em n que $\forall_{l<h} e(n,l) = n$ e $\forall_{l\geq h} e(n,l) = 0$. Para $n = 0$, trivial, porque MG_0 tem dimensão 0. Para $n = 1$, cada $e(1,l) \leq 1$, e $\sum_l e(1,l) = h$, logo $e(1,0) = \cdots = e(1,h-1) = 1$ e os restantes são 0. Supor $n \geq 2$. Logo, $e(n-1, l) = \min(n-1, e(n,l))$; para $l \geq h$, $0 = \min(n-1, e(n,l))$, logo $e(n,l) = 0$. Como $n \cdot h = \sum_{l=0}^{h-1} e(n,l) \leq h \cdot n$, vale $\forall_{l<h} e(n,l) = n$.

Portanto, como $W(k)$-módulos, $MG_n \cong W_n(k)^{\oplus h}$, e como $MG_{n+1} \to MG_n$ (ajustando os isomorfismos) é $r^{\oplus h} : W_{n+1}(k)^{\oplus h} \to W_n(k)^{\oplus h}$, vale $\lim_n MG_n \cong W(k)^{\oplus h}$ como $W(k)$-módulos, que é $W(k)$-livre de posto h. Provar que esse functor é antiequivalência é similar ao corolário 6.4.33. □

7.2 Módulos de Cartier

Agora denotamos por $\mathrm{MD}\, G$ os módulos de Dieudonné. Há um outro módulo $\mathrm{MC}\, G$ associado a esquemas-grupos p-divisíveis, que em certo caso (baseando-se em (Hedayatzadeh, 2020)) provaremos ser isomorfo a $\mathrm{MD}(G^{(*)})$.

Definição 7.2.1. Dado G esquema-grupo formal abeliano sobre k, define-se o "módulo de Cartier" como $\mathrm{MC}\, G \coloneqq \mathsf{Ab}^{k-\mathsf{Alg}}(\widehat{W}, G)$, com E-ação esquerda dada por: $\xi \cdot \phi \coloneqq (\phi \circ (\xi\cdot))$, $F \cdot \phi \coloneqq (\phi \circ V)$, $V \cdot \phi \coloneqq (\phi \circ F)$.

Lema 7.2.2. *Se G é p-divisível com cada G_n de álgebra de Hopf local, define-se E-linear* $\mathrm{MD}(G^{(*)}) \to \mathrm{MC}(G)$.

Demonstração. (De Hedayatzadeh (2020)) Temos que $\mathrm{MD}(G^{(*)}) = \lim_n \mathrm{MD}(G^*_n)$, e também $\mathrm{MD}(G^*_n) = \operatorname{co\lim}_m \mathsf{Ab}^{k-\mathsf{Alg}}(G^*_n, W_m)$ pois seu dual G^{**}_n tem álgebra de Hopf

local. Também, temos $\operatorname{co\lim}_m \mathsf{Ab}^{k-\mathsf{Alg}}(G_n^*, W_m) \cong \operatorname{co\lim}_m \mathsf{Ab}^{k-\mathsf{Alg}}(\widehat{W}^m, G_n)$ pelo teorema 6.2.12, lema 6.2.8; o primeiro diagrama de colimite tem mapas dados por $v : W_m \to W_{m+1}$, e o segundo tem mapas dados por seus duais $f : \widehat{W}^{m+1} \to \widehat{W}^m$. Seja $(x_n) \in \lim_n \mathrm{MD}(G_n^*)$; cada x_n corresponde a $[y_{n,N(n)} : \widehat{W}^{N(n)} \to G_n]$, algum $N(n) \geq n$; e $\mathrm{MD}(p^*)(x_{n+1}) = x_n$ implica $[(p\cdot)\circ y_{n+1,N(n+1)}] = [y_{n,N(n)}]$, isto é, $(p\cdot)\circ y_{n+1,N(n+1)}\circ f^{N(n)} = y_{n,N(n)} \circ f^{N(n+1)}$ em $\widehat{W}^{N(n)+N(n+1)}$.

Vale $y_{n,N(n)} \circ V^n \circ F^n = y_{n,N(n)} \circ p^n = 0$ porque p^n se anula em G_n. A sequência $\widehat{W}^{N(n)} \overset{F^n}{\to} \widehat{W}^{N(n)} \overset{f^{N(n)-n}}{\to} \widehat{W}^n \to 0$ é exata, pois é $\underline{\mathrm{Hom}}(, \boldsymbol{G_m})$ aplicada a $0 \to W_n \overset{v^{N(n)-n}}{\to} W_{N(n)} \overset{V^n}{\to} W_{N(n)}$, exata. Logo, $y_{n,N(n)} \circ V^n = \phi_n \circ f^{N(n)-n}$ para único $\phi_n : \widehat{W}^n \to G_n \to G$.

Também, $x_n = [y_{n,N(n)} \circ f^d : \widehat{W}^{N(n)+d} \to G_n]$, para cada $d \geq 0$, e um mapa $\phi : \widehat{W}^n \to G$ satisfaz $y_{n,N(n)} \circ f^d \circ V^n = \phi \circ f^{N(n)+d-n}$ sse $y_{n,N(n)} \circ V^n \circ f^d = \phi_n \circ f^{N(n)+d-n} = \phi \circ f^{N(n)+d-n}$, sse $\phi = \phi_n$. Então, temos o morfismo $\phi_n : \widehat{W}^n \to G$, que só depende de x_n, não de $N(n)$.

Usando $(p\cdot) = V \circ F$, denotando $i : G_n \to G_{n+1}$, vale $y_{n+1,N(n+1)} \circ f^{N(n)} \circ (V \circ F)\circ V^n = i\circ y_{n,N(n)}\circ f^{N(n+1)}\circ V^n$, logo $\phi_{n+1}\circ F\circ f^{N(n+1)+N(n)-(n+1)} = i\circ\phi_n\circ f^{N(n+1)+N(n)-n}$; como $f^d : \widehat{W}^{M+d} \to \widehat{W}^M$ é épica, pois é $\underline{\mathrm{Hom}}(, \boldsymbol{G_m})$ aplicada a $W_M \overset{v^d}{\to} W_{M+d}$, mônica, vale $\phi_{n+1} \circ F = i \circ \phi_n \circ f$; isto é, $i \circ \phi_n = (\phi_{n+1} \restriction \widehat{W}^n)$.

Então, temos $\phi \coloneqq (\bigcup_n \phi_n) : \widehat{W} \to G$. Pode-se ver que cada $x_n \mapsto \phi_n$ é aditiva, logo $(x_n)_n \mapsto \phi$ é aditiva. Resta mostrar E-linear. Vale $F \cdot (x_n)_n = (F \cdot x_n)_n$, com $F \cdot x_n$ correspondendo a $y_{n,N(n)} \circ V$ porque $\widehat{W}^{N(n)} \overset{V}{\to} \widehat{W}^{N(n)}$ é $\underline{\mathrm{Hom}}(, \boldsymbol{G_m})$ aplicado a $W_{N(n)} \overset{F}{\to} W_{N(n)}$; logo, $F \cdot x_n \mapsto \phi_n \circ V$, logo $F \cdot (x_n)_n \mapsto \phi \circ V$, que é $F \cdot \phi$; similarmente, $V \cdot (x_n)_n \mapsto \phi \circ F = V \cdot \phi$. Também, dado $\xi \in W(k)$, como $\langle u_0, \xi \cdot u_1\rangle = \langle \xi \cdot u_0, u_1\rangle$ (pareamento de vetores de Witt), o dual de $(\xi^{\sigma^{-N(n)}}\cdot) : W_{N(n)} \to W_{N(n)}$ é $(\xi^{\sigma^{-N(n)}}\cdot) : \widehat{W}^{N(n)} \to \widehat{W}^{N(n)}$ e $y_{n,N(n)} \circ (\xi^{\sigma^{-N(n)}}\cdot) \circ V^n = y_{n,N(n)} \circ V^n \circ (\xi^{\sigma^{-N(n)+n}}\cdot) = \phi_n \circ f^{N(n)-n} \circ (\xi^{\sigma^{-N(n)+n}}\cdot) = \phi_n \circ (\xi\cdot) \circ f^{N(n)-n}$, logo $\xi \cdot (x_n)_n \mapsto \phi \circ (\xi\cdot)$. □

Lema 7.2.3. *O mapa do lema anterior* $\mathrm{MD}(G^{(*)}) \to \mathrm{MC}(G)$ *é isomorfismo.*

Demonstração. Seja $(x_n)_n \in \lim_n \mathrm{MD}(G_n^*)$ no núcleo. Então, cada x_n corresponde a $[y_{n,N(n)} : \widehat{W}^{N(n)} \to G_n]$, e $y_{n,N(n)} \circ V^n = 0$. Logo, $y_{n,N(n)}$ escreve-se como $\widehat{W}^{N(n)} \to W_n^{N(n)} \overset{z_{n,N(n)}}{\to} G_n$. Como $\mathrm{MD}(p^*)(x_{n+1}) = x_n$, vale $(p\cdot) \circ z_{n+1,N(n+1)} \circ f^{N(n)} = z_{n,N(n)} \circ f^{N(n+1)} \circ r$. $(*)$

Antes de continuar, prova-se que cada $G_n \overset{F^n}{\to} G_n^{(p)^n} \overset{V^n}{\to} G_n$ é exata. (Aqui não é necessário G_n ser de tipo local). Pelo lema 5.1.8, a composta $G_n \overset{F}{\to} G_n^{(p)} \overset{V}{\to} G_n$ é igual a $p \restriction G_n$; similarmente $V^n \circ F^n = p^n = 0 \restriction G_n$. Agora, seja $x : (\cdots) \to G_n^{(p)^n}$ elemento generalizado com $V^n\circ x = 0$. Como $p^n : G_{2\cdot n}^{(p)^n} \to G_n^{(p)^n}$ é épica (porque $(\cdots)^{(p)^n}$ é equivalência da categoria a si mesma), existe elemento generalizado $y : (\cdots) \to G_{2\cdot n}^{(p)^n}$ com $(p^n\cdot) \circ y \equiv x$; logo, $(p^n\cdot) \circ (V^n \circ y) \equiv V^n \circ x = 0$, logo $V^n \circ y$ é da forma $(\cdots) \overset{z}{\to}$

$G_n^{(p)^n} \to G_{2\cdot n}^{(p)^n}$ (porque $(\cdots)^{(p)^n}$ preserva núcleos, como $\mathrm{nuc}(p^n : G_{2\cdot n} \to G_{2\cdot n}) \cong G_n$); logo, $i \circ F^n \circ (V^n \circ z) = F^n \circ (V^n \circ y) = i \cdot (p^n \cdot) \circ y \equiv i \cdot x$, logo $F^n \circ (\cdots) \equiv x$.

Dado n, mostra-se que há $M(n)$ com $\forall_{n' \geq M(n)} p^{n'-n} \cdot \mathrm{nuc}(V^{n'} : (\cdots) \to G_{n'}) = 0$. De fato, como G_n é de tipo local, há $M(n)$ com $F^{M(n)}$ anulando-se em G_n; logo, se $n' \geq M(n)$, $G_{n'} \overset{F^{n'}}{\to} G_{n'}^{(p)^{n'}} \overset{p^{n'-n}}{\to} G_n^{(p)^{n'}}$ é $G_{n'} \overset{p^{n'-n}}{\to} G_n \overset{F^{n'}}{\to} G_n^{(p)^{n'}}$, zero, logo pelo parágrafo anterior, $p^{n'-n} \cdot \mathrm{nuc}(V^{n'} : (\cdots) \to G_{n'}) = 0$.

Quer-se agora mostrar $z_{n,N(n)} = 0$. Pelo parágrafo anterior, há $n' \geq n$ com $p^{n'-n} \cdot \mathrm{nuc}(V^{n'} : (\cdots) \to G_{n'}) = 0$; usando $z_{n,N(n)} \circ f^{N(n')} \circ r^{n'-n} = (p^{n'-n} \cdot) \circ z_{n',N(n')} \circ f^{N(n)}$, que é a condição $(*)$ repetida (e com algumas aplicações da épica f removidas), vale $V^{n'} \circ z_{n',N(n')} = z_{n',N(n')}^{(p)^{-n'}} \circ V^{n'} = 0$ em $W_{n'}^{N(n')}$, logo $z_{n',N(n')}$ fatora-se pelo núcleo de $V^{n'}$, e assim $(p^{n'-n} \cdot) \circ z_{n',N(n')} = 0$; logo, $z_{n,N(n)} = 0$. Conclui-se $x_n = 0$, e temos a injetividade.

Queremos mostrar a sobrejetividade. Seja $\phi : \widehat{W} \to G$. Há restrições $\widehat{W}^n \to G$, e como p^n se anula em $\widehat{W}^n$, há fatorações $\widehat{W}^n \overset{\phi_n}{\to} G_n \to G$. Há $N(n) \geq n$ com $p^{N(n)-n} \cdot \mathrm{nuc}(V^{N(n)} : (\cdots) \to G_{N(n)})$; SPDG cada $N(n+1)$ é tão grande que $N(n+1) \geq N(n)$. Pela antiequivalência à categoria dos esquemas-grupos formais abelianos, há F e V naturais nessa categoria, estendendo F e V da categoria dos finitos. Logo, $0 = \phi_n \circ F^n = F^n \circ \phi_n^{(p)^{-n}}$. Como também $(\cdots) \overset{V^n}{\to} (\cdots) \overset{F^n}{\to} (\cdots)$ é exata, sendo $\overline{G}_n$ a "imagem" de $V^n : G_n \to G_n^{(p)^{-n}}$ (isto é, conúcleo do núcleo), temos fatoração $\overline{\phi}_n : \widehat{W}^n \to \overline{G}_n$ de $\phi_n^{(p)^{-n}} : \widehat{W}^n \to G_n^{(p)^{-n}}$. Como $p^{N(n)-n} : G_{N(n)} \to G_n$ também anula $\mathrm{nuc}(V^{N(n)} : G_{N(n)} \to (\cdots))$, existe fatoração $\pi_n : \overline{G}_{N(n)} \to G_n$ de $p^{N(n)-n}$. Define-se $y_{n,N(n)} : \widehat{W}^{N(n)} \to G_n$ como $\pi_n \circ \overline{\phi}_{N(n)}$.

Noutras palavras: dado elemento generalizado $x : (\cdots) \to \widehat{W}^{N(n)}$, há $x' : (\cdots) \to G_{N(n)}$ com $\phi_{N(n)}^{(p)^{-N(n)}} \circ x \equiv V^{N(n)} \circ x'$, e independentemente da opção x', vale $y_{n,N(n)} \circ x \equiv (p^{N(n)-n} \cdot) \circ x'$.

Quer-se provar $(p\cdot) \circ y_{n+1,N(n+1)} \circ f^{N(n)} = y_{n,N(n)} \circ f^{N(n+1)}$: dado elemento generalizado $x : (\cdots) \to \widehat{W}^{N(n+1)+N(n)}$, abrevie $x_{N(n+1)} \coloneqq f^{N(n)} \circ x$ e $x_{N(n)} \coloneqq f^{N(n+1)} \circ x$; há $x'_{N(n+1)} : (\cdots) \to G_{N(n+1)}$ com $\phi_{N(n+1)}^{(p)^{-N(n+1)}} \circ x_{N(n+1)} \equiv V^{N(n+1)} \circ x'_{N(n+1)}$; e, usando $N(n+1) \geq N(n)$, sendo $x'_{N(n)} \coloneqq (p^{N(n+1)-N(n)} \cdot) \circ x'_{N(n+1)}$, vale $i \circ V^{N(n)} \circ x'_{N(n)} = F^{N(n+1)-N(n)} \circ V^{N(n+1)} \circ x'_{N(n+1)} \equiv \phi_{N(n+1)}^{(p)^{-N(n)}} \circ F^{N(n+1)-N(n)} \circ x_{N(n+1)} = i \circ \phi_{N(n)}^{(p)^{-N(n)}} \circ f^{N(n+1)-N(n)} \circ x_{N(n+1)} = i \circ \phi_{N(n)}^{(p)^{-N(n)}} \circ x_{N(n)}$; então, $(p\cdot) \circ y_{n+1,N(n+1)} \circ x_{N(n+1)} \equiv (p^{N(n+1)-n} \cdot) \circ x'_{N(n+1)} = (p^{N(n)-n} \cdot) \circ x'_{N(n)} \equiv y_{n,N(n)} \circ x_{N(n)}$.

Logo, os $[y_{n,N(n)} : \widehat{W}^{N(n)} \to G_n]$ correspondem a elemento de $\lim_n \mathrm{MD}(G_n)$. Resta provar que a imagem é ϕ. Para tal, queremos provar $y_{n,N(n)} \circ V^n = \phi_n \circ f^{N(n)-n}$. Seja $x^{(p)^n} : (\cdots) \to \widehat{W}^{N(n)}$ elemento generalizado. Vale $y_{n,N(n)} \circ V^n \circ x^{(p)^n} = V^n \circ y_{n,N(n)}^{(p)^n} \circ x^{(p)^n}$; há $x' : (\cdots) \to G_{N(n)}$ com $\phi_{N(n)}^{(p)^{-N(n)}} \circ x \equiv V^{N(n)} \circ x'$, e $y_{n,N(n)} \circ x \equiv (p^{N(n)-n} \cdot) \circ x'$; logo, $i \circ V^n \circ y_{n,N(n)}^{(p)^n} \circ x^{(p)^n} \equiv i \circ V^n \circ (p^{N(n)-n} \cdot) \circ (x')^{(p)^n} = F^{N(n)-n} \circ V^{N(n)} \circ (x')^{(p)^n} \equiv F^{N(n)-n} \circ \phi_{N(n)}^{(p)^{n-N(n)}} \circ x^{(p)^n} = \phi_{N(n)} \circ F^{N(n)-n} \circ x^{(p)^n} = i \circ \phi_n \circ f^{N(n)-n} \circ x^{(p)^n}$. □

7.3 Uso com torções de variedades abelianas

De (Mumford, 1974)II.(4,6), se S é uma "variedade abeliana" (isto é, objeto-grupo abeliano na categoria dos "conjuntos algébricos projetivos" sobre um corpo algebricamente fechado de característica p, que seja irredutível), então o seguinte esquema-formal é p-divisível de altura $2 \cdot \dim S$ (onde $\dim S$ é "dimensão de Krull"): $G \coloneqq \bigcup_{n\geq 0} G_n$, $G_n \coloneqq \mathrm{nuc}(p^n : S \to S)$; este núcleo é na categoria de "esquemas-grupos abelianos", e pode ser provado estar na subcategoria dos afins finitos. (Sem provas aqui).

De (Demazure, 1972)IV.4 (teorema de Íuriĭ Mánin), se $k = \overline{k}$ de característica p, todo $\operatorname{Frac} W(k)$-espaço vetorial de dimensão finita com E-ação esquerda compatível X é isomorfo a uma soma direta dos $X^{s/r} \coloneqq \operatorname{Frac} W(k) \otimes_{\mathbb{Q}_p} \mathbb{Q}_p[T]/(T^r - p^s)$, para $0 \leq \frac{s}{r} \leq 1$ fração reduzida, onde $\mathbb{Q}_p$ é o corpo p-ádico; tem base $1 \otimes T^0, \ldots, 1 \otimes T^{r-1}$; a ação de F é $(T\cdot)$, injetiva logo bijetiva, e a ação de V é $p \cdot F^{-1}$. Por exemplo, se $\dim_{\operatorname{Frac} W(k)} X = 2$, então X é isomorfo a $X^0 \oplus X^0$, $X^1 \oplus X^1$, $X^0 \oplus X^1$ ou $X^{1/2}$.

Dados dois esquemas-grupos p-disivíveis G e G' de mesma altura, temos que $\operatorname{Frac} W(k) \otimes \operatorname{MD} G \cong \operatorname{Frac} W(k) \otimes \operatorname{MD} G'$ sse há $\operatorname{Frac} W(k) \otimes \operatorname{MD} G \to \operatorname{Frac} W(k) \otimes \operatorname{MD} G'$ injetivo (pois as dimensões coincidem), e há N tal que esse mapa multiplicado por p^N induz $\operatorname{MD} G \to \operatorname{MD} G'$; assim, $\operatorname{Frac} W(k) \otimes \operatorname{MD} G \cong \operatorname{Frac} W(k) \otimes \operatorname{MD} G'$ sse há injetivo (mônico) $\operatorname{MD} G \to \operatorname{MD} G'$ de conúcleo de k-dimensão finita, sse há épico $G' \to G$ de núcleo finito. (Esta condição é dita "isogenia").

E de (Demazure, 1972)V.3, ainda supondo $k = \overline{k}$ de característica p, se S é uma variedade abeliana, associada a p-divisível $\overline{S}$, então $\operatorname{Frac} W(k) \otimes \operatorname{MD} \overline{S}$ é isomorfo a alguma soma $X^{\lambda_1} \oplus \cdots \oplus X^{\lambda_m}$ (ordem crescente λ_i) satisfazendo $\lambda_i + \lambda_{m+1-i} = 1$; assim, $\overline{S}$ é isógeno a algum $G^{\lambda_1} \oplus \cdots \oplus G^{\lambda_m}$. E se adicionalmente a sequência $\lambda_\bullet$ é $(0, \ldots, 0, 1/2, 1, \ldots, 1)$, então essa isogenia é um isomorfismo; é o que ocorre com $\dim S = 1$, por exemplo, para "curvas elípticas".

Bibliografia

Bourbaki, Nicolas (1985). *Algèbre Commutative*. Vol. Ch. 1–4. Éléments de Mathématique. Springer.

Demazure, Michel (1972). *Lectures on p-Divisible Groups*. Springer-Verlag.

Demazure, Michel e Pierre Gabriel (1970). *Géométrie Algébrique, Généralités, Groupes Commutatifs*. Vol. I. Groupes Algébriques. Masson Cie Éditeur e North-Holland Publishing Company.

Hedɑyatzɑdeh, S. Mohammad Hɑdi (2020). "Explicit Isomorphism between Cartier and Dieudonné Modules". Em: *Journal of Algebra. Elsevier*. DOI: https://doi.org/10.1016/j.jalgebra.2020.12.008.

Mac Lane, Saunders (1998). *Categories for the Working Mathematician*. Springer-Verlag.

Milne, James S (2015). *Algebraic Groups*. URL: https://www.jmilne.org/math/CourseNotes/ala.html.

Mumford, David (1974). *Abelian Varieties*. Oxford University Press.

Riehl, Emily (2016). *Category Theory in Context*. Dover Publications. URL: https://emilyriehl.github.io/files/context.pdf.

Sweedler, Moss (1969). *Hopf Algebras*. W. A. Benjamin.

Takeuchi, Mitsuhiro (1972). "A Correspondence between Hopf Ideals and Sub-Hopf Algebras". Em: *Manuscripta Mathematica. Springer-Verlag*. DOI: https://doi.org/10.1007/BF01579722.

Waterhouse, William C (1979). *Introduction to Affine Group Schemes*. Springer-Verlag.