Universidade Estadual de Campinas - UNICAMP

Instituto de Matemática, Estatística

e Computação Científica

Departamento de Matemática

Grupos algébricos e Hiperálgebras

Tiago Macedo

Dissertação de mestrado orientada pelos professores
Dr. Adriano Moura e Dr. Marcos Jardim

Grupos Algébricos e Hiperálgebras.

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Tiago Rodrigues Macedo e aprovada pela comissão julgadora.

Campinas, 19 de Fevereiro de 2009.

Prof. Dr:. Adriano Adrega de Moura
Orientador

Prof. Dr:. Marcos Benevenuto Jardim
Co-orientador

Banca Examinadora:

1. Prof. Dr. Adriano Adrega de Moura.
2. Prof. Dr. Plamen Emilov Kuschloukov.
3. Prof. Dr. Eduardo de Sequeira Esteves.

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de MESTRE em matemática.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Crisllene Queiroz Custódio – CRB8 / 7966

	Macedo, Tiago Rodrigues
M13g	Grupos algébricos e hiperálgebras / Tiago Rodrigues Macedo -- Campinas, [S.P. : s.n.], 2009.
	Orientador : Adriano Adrega de Moura ; Marcos Benevenuto Jardim
	Dissertação (Mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.
	1. Chevalley, Grupos de. 2. Algebra de Hopf. 3. Lie, Algebras de. I. Moura, Adriano Adrega de. II. Jardim, Marcos Benevenuto. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

Título em inglês: Algebraic groups and hyperalgebras

Palavras-chave em inglês (Keywords): 1. Chevalley Groups. 2. Hopf algebras. 3. Lie Algebras.

Área de concentração: Álgebra

Titulação: Mestre em Matemática

Banca examinadora: Prof. Dr. Adriano Adrega de Moura (IMECC-UNICAMP)
Prof. Dr. Plamen Emilov Kuschlukov (IMECC-UNICAMP)
Prof. Dr. Eduardo de Sequeira Esteves (IMPA)

Data da defesa: 19/02/2009

Programa de Pós-Graduação: Mestrado em Matemática

Dissertação de Mestrado defendida em 19 de fevereiro de 2009 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

____

Prof. (a). Dr (a). ADRIANO ADREGA DE MOURA

____

Prof. (a). Dr (a). PLAMEN EMILOV KOCHLOUKOV

____

Prof. (a). Dr (a). EDUARDO DE SEQUEIRA ESTEVES

Resumo

Apresentaremos resultados relacionando a álgebra de distribuições de grupos de Chevalley com as chamadas hiperálgebras. Estas últimas são álgebras de Hopf construídas por redução módulo p da forma integral de Kostant para álgebras de Lie simples. Em seguida, tentamos, a partir de uma certa classe de álgebras de Hopf, a saber, álgebras de Hopf que são álgebras de distribuições de grupos algébricos, reconstruir esses grupos algébricos.

Abstract

We present some results which relate the algebra of distributions of a Chevalley group and the so called hyperalgebras. The latter are Hopf algebras obtained by reduction modulo p of the Kostant integral form of a simple Lie algebra. Then we try to rebuild algebraic groups from Hopf algebras which are their algebras of distribution.

Agradecimentos

Durante os dois anos em que o processo de mestrado ocorreu, muitas pessoas exerceram alguma influência sobre mim e consequentemente sobre essa dissertação. A todas essas pessoas, ao CNPq e a CAPES eu gostaria de agradecer. Em particular, algumas dessas pessoas, eu gostaria de listar. O pessoal da república na qual eu morei, em especial o Lonardo pela peciência, pela compreensão e pelo carinho. O pessoal da secretaria de pós-graduação do IMECC, porque se não fosse por eles, eu não teria conseguido chegar até o fim. O Rafael Leão, o Dirceu, a Cíntia, o Tomás, o Francis, a Deborah pela amizade. Minha irmã pelos conselhos sábios, pela compreensão e pelo amor. Os professores do IMECC, em particular, o Marcos Jardim e o Adriano. Ao Marcos, eu devo a chance de estudar um pouco de geometria algébrica. Ao Adriano, eu devo muito mais do que o conteúdo matemático. Durante esses dois anos, ele me ensinou a encarar as coisas de uma maneira muito mais responsável e pragmática. Eu devo agradecer a ele pela imensa paciência comigo, pela quantidade não enumerável de conselhos e pela atenção.

A meus pais. Se eu estou aqui, é por causa deles.

Tiago,
Fevereiro de 2009.

Desencanto

Eu faço versos como quem chora
De desalento, de desencanto
Fecha meu livro se por agora
Não tens motivo algum de pranto.

Meu verso é sangue, volúpia ardente
Tristeza esparsa, remorso vão
Dói-me nas veias amargo e quente
Cai gota à gota do coração.

É nesses versos de angústia rouca
Assim dos lábios a vida corre
Deixando um acre sabor na boca
Eu faço versos como quem morre.
(Manuel Bandeira)

Conteúdo

Introdução

Grupos de Lie e álgebras de Lie são duas estruturas relacionadas que têm aplicações em muitas áreas da matemática e da física. Um grupo de Lie é um conjunto que ao mesmo tempo tem estrutura de variedade diferenciável e de grupo. A álgebra de Lie de um grupo de Lie, por sua vez, é o espaço tangente no ponto identidade à variedade subjacente ao grupo de Lie. Como estes dois objetos estão intimamente relacionados, as álgebras de Lie são uma ferramenta muito importante para entender a estrutura dos grupos de Lie. Um exemplo desta relação tão estreita é a existência de uma bijeção entre o conjunto de subgrupos conexos e simplesmente conexos de um grupo de Lie complexo e o conjunto de subálgebras da sua álgebra de Lie. Outro exemplo é a existência de uma bijeção entre o conjunto de representações diferenciáveis de um grupo de Lie complexo e o conjunto de representações de dimensão finita de sua álgebra de Lie.

Como os grupos de Lie são variedades diferenciáveis, as ferramentas usadas no seu estudo advêm da Geometria Diferencial e da Topologia Diferencial. Uma categoria análoga à dos grupos de Lie é a categoria dos *grupos algébricos*. Em particular, todo grupo algébrico complexo munido da topologia induzida pela topologia usual de $\mathbb{C}$ é um grupo de Lie. Grupos algébricos são conjuntos que concomitantemente têm estruturas de variedade algébrica e grupo. Por isso as ferramentas utilizadas no estudo dos grupos algébricos advêm principalmente da Geometria Algébrica.

Afim de entender a relação entre grupos algébricos e suas álgebras de Lie sobre corpos arbitrários, nas décadas de cinquenta e sessenta, Dieudonné [Die] e Chevalley [Che1] introduziram e desenvolveram a *hiperálgebra* de uma álgebra de Lie e a *álgebra de distribuições* de um grupo algébrico. Em característica positiva, esta hiperálgebra tem papel análogo ao que a álgebra universal envelopante da álgebra de Lie do grupo algébrico tinha em característica zero. A álgebra universal envelopante e a hiperálgebra são duas álgebras associativas naturalmente associadas à álgebra de Lie. A álgebra de distribuições, por sua vez, é uma álgebra associativa que está associada ao grupo algébrico e que ajuda a entender como o grupo se comporta nas vizinhanças do ponto identidade.

Tentando entender a relação entre um grupo algébrico G, sua álgebra de distribuições $D(G)$, sua álgebra de Lie $\mathfrak{g}$ e sua hiperálgebra $hy(\mathfrak{g})$, no fim da década de setenta, Sullivan [Sul] e Yanagihara [Yan] mostraram que sob certas condições existe uma bijeção entre o conjunto de representações de G, o conjunto de representações de sua álgebra de distribuições $D(G)$ e o conjunto das representações de sua hiperálgebra $hy(\mathfrak{g})$.

No caso complexo, o processo usado para obter a álgebra de Lie de um grupo algébrico (de Lie) é a diferenciação no ponto identidade do grupo. O processo inverso, usado para obter o grupo algébrico da álgebra de Lie, é a exponenciação. No caso de característica positiva, este último processo não pode ser realizado. Esta é a motivação para a construção de um grupo algébrico análogo àquele obtido por exponenciação da álgebra de Lie em característica zero. Grupos assim construídos são chamados de *Grupos de Chevalley.*

Os dois principais objetivos desta dissertação de mestrado são:

(i) Entender e reescrever a demonstração de que sob certas condições a álgebra de distribuições de um grupo de Chevalley é isomorfa à hiperálgebra de sua álgebra de Lie. Este resultado, que une as duas pontas da teoria, já foi mostrado por Haboush no artigo [Hab] e por Cline, Parshall e Scott no artigo [CPS].

(ii) Entender quais álgebras associativas são álgebras de distribuição de algum grupo algébrico e como reconstruir o grupo algébrico a partir de sua álgebra de distribuições.

A motivação para o estudo acima vem da pesquisa do orientador desta dissertação sobre as chamadas hiperálgebras de laços. Moralmente estas álgebras devem estar relacionadas aos grupos de laços de maneira similar àquela descrita acima entre as hiperálgebras e os grupos de Chevalley. Porém, em dimensão infinita a teoria clássica de geometria algébrica não funciona como no caso de dimensão finita e, por isso, é necessário lançar mão de outros pontos de vista a fim de desenvolver resultados análogos àqueles conhecidos para os grupos algébricos (de dimensão finita). Gostaríamos, por exemplo, de obter análogos a resultados cohomológicos como o resultado conhecido como "Teorema do Cancelamento de Kempf" no contexto de variedades bandeira de grupos de laços associados a subálgebras parabólicas que não são a subálgebra de Borel padrão. Acreditamos que para tratar os grupos algébricos simplesmente conexos o ponto de vista funtorial, através do funtor representável construído a partir da hiperálgebra, seja um ponto de vista viável para ser estendido ao contexto de dimensão infinita. Isto é, partindo-se da hiperálgebra de laços, considera-se o grupo de laços que, por definição, é dado pelo funtor de esquema de grupos representado pela hiperálgebra de laços e tenta-se desenvolver a teoria toda para estes funtores.

O texto está dividido em quatro capítulos. O primeiro capítulo contém uma breve revisão dos pré-requisitos que serão necessários ao longo do texto. A primeira seção deste capítulo, que é baseada em [Ati] e [Eis], trata de álgebra comutativa. O material não vai além de um curso introdutório no assunto. A segunda seção trata de álgebras de Hopf. Ela cobre apenas uma introdução ao assunto e é baseada em [Mon]. A terceira seção contém as noções básicas da teoria de álgebras de Lie. Este material é basicamente de [Jac]. A quarta e última seção deste capítulo provê uma introdução à teoria de categorias, basicamente funtores e construções universais que serão usadas nas definições de feixes e stalks no terceiro capítulo. A referência para este capítulo é o livro clássico [Mac], mas a apresentação segue [Ana].

O segundo capítulo se aprofunda mais na teoria de álgebras de Lie. Este material é essencial para entender a estrutura dos grupos de Chevalley no quarto capítulo. A referência principal para este segundo capítulo é [Hum1].

O terceiro capítulo trata de noções básicas de geometria algébrica. Na primeira seção introduz-se as variedades afins. Na segunda seção, discute-se sobre morfismos entre variedades afins e sobre a equivalência entre as categorias de variedades afins e de álgebras finitamente geradas e reduzidas. As terceira e quarta seções são análogas às duas primeiras, mas tratam do caso projetivo. Na quinta seção define-se variedade algébrica do ponto de vista clássico. Na sexta seção, introduz-se feixes e esquemas para redefinir variedades algébricas nesta linguagem. A sétima seção trata de funtores, que será uma outra forma de entender as variedades algébricas. A próxima seção trata da dimensão de variedades e a última seção deste capítulo trata de espaços tangentes a variedades afins, pois este conceito será importante no capítulo seguinte. Este capítulo é baseado em [Hum2], [Har] e [Jan].

O quarto capítulo é sobre grupos algébricos. Na primeira seção definimos e mostramos algumas propriedades básicas dos grupos algébricos. Na segunda, definimos álgebra de Lie de um grupo algébrico. A terceira seção contém uma discussão sobre álgebras de Hopf associadas naturalmente a grupos algébricos. Na quarta seção são definidas e mostradas propriedades sobre hiperálgebras. A quinta seção é dedicada ao estudo dos grupos de Chevalley. Nesta seção, também é provado um importante teorema que relaciona as álgebras de distribuições às hiperálgebras. Este capítulo é baseado em [Hum2], [Jan], [Ste], [Hab], [CPS] e [Kos].

Capítulo 1

Pré-requisitos

1.1 Notação básica

Nesse texto denotar-se-á por $\mathbb{C}$ o corpo dos números complexos, por $\mathbb{R}$ o corpo dos números reais, por $\mathbb{Q}$ o corpo dos números racionais, por $\mathbb{Z}$ o anel dos números inteiros e por $\mathbb{N}$ o conjunto (monoide) $\{0, 1, 2, 3, \ldots\}$ de números naturais. Para qualquer conjunto X com estrutura de monoide aditivo, $X \setminus \{0\}$ será denotado por $X^{\bullet}$. Além disso, os isomorfismos serão denotados por $\simeq$.

1.2 Álgebra Comutativa

Essa seção tem como objetivo expor as definições e os fatos (sem demonstrações) sobre álgebra comutativa que serão usados mais tarde no resto do texto. As definições e os resultados foram retirados de [Ati] e [Eis].

Definição 1.2.1. Um *anel* é um conjunto R munido de :

(i) uma estrutura de grupo abeliano com relação a adição, usualmente denotada por $+$;

(ii) uma função binária, associativa e distributiva sobre a adição, chamada de *multiplicação* e usualmente denotada por $\cdot$.

Quando a multiplicação é uma operação comutativa, chama-se o anel de *comutativo*. Quando existe um elemento $e_R \in R$, tal que $e_R.r = r.e_R = r$, para todo $r \in R$, e_R é chamado de *elemento neutro* da multiplicação e o anel é chamado de *anel com unidade*.

A partir de agora, os anéis considerados serão comutativos com unidade, a menos que seja dito o contrário.

Exemplo 1.2.2. Os principais exemplos de anéis são:

(i) Os números inteiros $\mathbb{Z}$. (O conjunto de números naturais $\mathbb{N}$ não forma um anel.)

(ii) Dado um anel R, o conjunto $R[x_1, \ldots, x_n] = \{f(x_1, \ldots, x_n) = \sum a_{k_1,\ldots,k_n} x_1^{k_1} \ldots x_n^{k_n} \mid a_{k_1,\ldots,k_n} \in R,\ \forall\ (k_1, \ldots, k_n) \in \mathbb{N}^n\}$, munido das operações usuais de polinômios, é chamado de *anel de polinômios sobre R*.

Definição 1.2.3. Seja R um anel. Os elementos $r \in R$ que têm inverso multiplicativo são chamados de *unidades do anel*. O conjunto de unidades do anel R é denotado por $R^{\times}$.

Um anel em que todo elemento, exceto o elemento neutro da adição, tem inverso multiplicativo é chamado de *corpo*.

Definição 1.2.4. Seja R um anel. Um elemento $r \in R$ é chamado de *divisor de zero* quando existe $s \in R^{\bullet}$, tal que $r.s = 0$. Um anel é um *domínio* quando o único divisor de zero é o elemento neutro da adição.

Definição 1.2.5. Um *subanel* de um anel R é um subconjunto $S \subseteq R$ que é um anel com as operações herdadas de R, ou seja, se $(R, +, \cdot)$ é anel, então $(S, +, \cdot)$ também é anel.

Um *ideal* de um anel R é um subgrupo aditivo $I \subseteq R$, tal que, para quaisquer $r \in R$ e $i \in I$, $ri \in I$. Um ideal $I \subseteq R$ é *não trivial* quando $I \neq \{0\}$ e é *próprio* quando $I \neq R$.

Da definição acima, conclui-se que se um ideal I de um anel R tiver uma unidade do anel R, então $I = R$. Em particular, ideais próprios e não triviais não são subanéis.

Como um ideal de um anel é um subgrupo aditivo do anel, então faz sentido considerar o quociente do anel pelo ideal.

Definição 1.2.6. Sejam R um anel e $I \subseteq R$ um ideal. Define-se o *anel quociente* de R por I, R/I, como o conjunto de classes laterais $\{r + I \mid r \in R\}$, onde:

(i) $r + I = s + I$, quando $r - s \in I$;

(ii) a adição $+$ é definida por: $(r + I) + (s + I) = (r + s) + I$, para todo $r, s \in R$;

(iii) a multiplicação $\cdot$ é definida por: $(r + I).(s + I) = (r.s) + I$, para todo $r, s \in R$.

Definição 1.2.7. Um ideal próprio $P \subseteq R$ é chamado de *primo* quando, para quaisquer $a, b \in R$, $a.b \in P$ implica $a \in P$ ou $b \in P$. Um ideal próprio $M \subseteq R$ é chamado de *maximal* quando, para qualquer ideal $I \subseteq R$, $M \subsetneq I$ implica $I = R$.

Proposição 1.2.8. Seja R um anel.

(i) Um ideal $P \subseteq R$ é primo se, e somente se, o anel quociente R/P é um domínio.

(ii) Um ideal $M \subseteq R$ é maximal se, e somente se, o anel quociente R/M é um corpo.

Definição 1.2.9. Um *morfismo de anéis* (com unidade) é uma função entre dois anéis $\varphi : R \to S$ que respeita a estrutura dos anéis, ou seja, para quaisquer $r, s \in R$:

(i) $\varphi(r + s) = \varphi(r) + \varphi(s)$;

(ii) $\varphi(r.s) = \varphi(r).\varphi(s)$;

(iii) $\varphi(e_R) = e_S$.

Um *endomorfismo* é um morfismo de um anel nele mesmo. Um *isomorfismo* é um morfismo bijetor de anéis.

Definição 1.2.10. Seja $\varphi : R \to S$ um morfismo de anéis.

(i) O *núcleo de* φ é o conjunto $ker(\varphi) = \{r \in R \mid \varphi(r) = 0\}$.

(*ii*) A *imagem de* φ é o conjunto $im(\varphi) = \{s \in S \mid \exists\ r \in R$, tal que $\varphi(r) = s\}$.

Teorema 1.2.11. Seja $\varphi : R \to S$ um morfismo de anéis, então:

(*i*) $\ker(\varphi)$ é ideal de R;

(*ii*) $R/\ker(\varphi) \simeq im(\varphi)$.

O teorema acima é conhecido como *Teorema do isomorfismo*.

Definição 1.2.12. Um anel é dito *local*, quando possui um único ideal maximal.

Definição 1.2.13. Sejam I_α, $\alpha \in A$, ideais de um anel R.

(*i*) Define-se a *soma dos ideais* I_α como o conjunto $\sum_{\alpha \in A} I_\alpha$ de elementos de R da forma $\sum_{\alpha \in A} i_\alpha$, onde $i_\alpha \in I_\alpha$, $\forall\ \alpha \in A$, e i_α é zero exceto para α em um subconjunto finito de A.

(*ii*) Define-se o *produto* (finito) de ideais $I_{\alpha_1} \ldots I_{\alpha_n}$, $\alpha_1, \ldots, \alpha_n \in A$, como o conjunto de elementos de R que são somas finitas de elementos da forma $i_{\alpha_1} \ldots i_{\alpha_n}$, onde $i_{\alpha_k} \in I_{\alpha_k}$, $\forall\ k = 1, \ldots, n$.

Proposição 1.2.14. Seja R um anel.

(*i*) Somas, interseções e produtos finitos de ideais em R são ideais em R.

(*ii*) Sejam I_α, $\alpha \in A$, ideais de um anel R. O ideal soma, $\sum_{\alpha \in A} I_\alpha$, é o menor ideal de R contendo I_α, $\forall\ \alpha \in A$. Por outro lado, o ideal intersecção, $\bigcap_{\alpha \in A} I_\alpha$, é o maior ideal em R contido em I_α, $\forall\ \alpha \in A$.

Proposição 1.2.15. Seja R um anel.

(*i*) Se um ideal $I \subseteq R$ está contido numa união finita de ideais primos de R, então I está contido em algum desses ideais primos.

(*ii*) Se um ideal primo $P \subseteq R$ contém uma intersecção finita de ideais de R, então P contém algum desses ideais.

Definição 1.2.16. Seja $I \subseteq R$ um ideal do anel R. Define-se o *radical* de I como o conjunto $\sqrt{I} = \{r \in R \mid\ \exists\ n \in \mathbb{N}^\bullet$, tal que $r^n \in I\}$. Quando $\sqrt{I} = I$, o ideal I é chamado de *radical*.

Proposição 1.2.17. Sejam R um anel e $I \subseteq R$ um ideal.

(*i*) O radical de I é um ideal de R.

(*ii*) O radical de I é a intersecção de todos os ideais primos de R que contem I. Em particular, se I for um ideal primo, então I é radical.

Definição 1.2.18. Seja R um anel. Define-se um conjunto A como uma R-*álgebra*, quando A for um anel não necessariamente comutativo e não necessariamente com unidade, munido de um morfismo de anéis $f : R \to A$.

Em geral, consideraremos álgebras comutativas com unidade, a menos de menção contrária.

Observação 1.2.19. Um anel A é uma R-álgebra se, e somente se, existe uma função binária $\mu : R \times A \to A$ satisfazendo, para quaisquer $a, a_1, a_2 \in A$ e $r, r_1, r_2 \in R$:

(i) $\mu(r, a_1 + a_2) = \mu(r, a_1) + \mu(r, a_2)$

(ii) $\mu(r_1, \mu(r_2, a)) = \mu(r_1 r_2, a)$

(iii) $\mu(r_1 + r_2, a) = \mu(r_1, a) + \mu(r_2, a)$

(iv) $\mu(e_R, a) = a$.

Na definição 1.2.18 acima, $\mu(r, a) = f(r).a$ satisfaz as condições da observação 1.2.19. Por outro lado, uma função satisfazendo as condições da observação 1.2.19 induz um morfismo de anéis $r \mapsto \mu(r, 1)$. Portanto, uma R-álgebra A pode ser vista também como um anel munido de uma multiplicação por elementos de R.

Quando R é um corpo, o morfismo de anéis $f : R \to A$ é injetor, pois caso contrário o núcleo de f seria um ideal não trivial de R, ou seja, $\ker(f) = R$. Nesse caso é possível ver R como subanel de A e μ como a restrição da multiplicação do anel A.

Definição 1.2.20. Sejam R um anel, A, B duas R-álgebras. Um *morfismo de R-álgebras* e um morfismo de anéis $\varphi : A \to B$ que satisfaz $\varphi(r.a) = r.\varphi(a)$ para todo $r \in R, a \in A$.

Definição 1.2.21. Seja R um anel. Um grupo abeliano M é um *R-módulo* quando existir uma operação binária $\cdot : R \times M \to M$, tal que, para quaisquer $r, r_1, r_2 \in R$ e $m, m_1, m_2 \in M$:

(i) $r.(m_1 + m_2) = r.m_1 + r.m_2$

(ii) $r_1.(r_2.m) = (r_1 r_2).m$

(iii) $(r_1 + r_2).m = r_1.m + r_2.m$

(iv) $e_R.m = m$.

Tal operação $\cdot$ é chamada de *ação de R em M*.

Sejam M, N dois R-módulos. Um *morfismo de R-módulos* é um homomorfismo de grupos abelianos $\varphi : M \to N$, que satisfaz $\varphi(r.m) = r.\varphi(m)$ para todo $r \in R, m \in M$. Analogamente, um *endomorfismo de módulos* é um morfismo de módulos de M para M e um *isomorfismo* é um endomorfismo bijetor de M para M.

Observe que, quando R é um corpo, um R-módulo é, por definição, um R-espaço vetorial. Observe também que toda R-álgebra é um R-módulo (pela observação 1.2.19).

Exemplo 1.2.22. Considere um anel R e um R-módulo M. O conjunto $End(M)$ de endomorfismos de M é munido de estrutura de R-álgebra (não comutativa). De fato, considere $T, S \in End(M)$, $(T+S)$ definido por $(T+S)(m) = T(m)+S(m)$, $m \in M$, é um endomorfismo de M. Da mesma forma, TS definido por $TS(m) = T \circ S(m)$, $m \in M$, é um endomorfismo de M. Para completar a estrutura de álgebra, considere $T \in End(M)$ e $r \in R$. Defina $r.T$ como $(r.T)(m) = r.T(m)$, $m \in M$.

Em particular, quando R é um corpo e V é um R-espaço vetorial, $End(V)$ é uma R-álgebra.

Definição 1.2.23. Sejam R um anel, A uma R-álgebra e M um R-módulo. Um morfismo de álgebras $\rho : A \to End(M)$ é chamado de *representação de A em M*.

Observe que para todo anel R e todo R-módulo M, a ação de R em M induz uma representação de R em M. Explicitamente, a representação $\rho : R \to End(M)$ é dada por $\rho(r)(m) = r.m$, $\forall\, r \in R, m \in M$. Por outro lado, uma representação $\rho : A \to End(M)$ de uma R-álgebra A em M induz uma outra estrutura de módulo em M. Explicitamente, $a.m = \rho(a)(m)$, $\forall\, a \in A, m \in M$.

Definição 1.2.24. Sejam R um anel e M um R-módulo. Um subconjunto $N \subseteq M$ é um *submódulo* de M quando N for um R-módulo com as estruturas (de grupo abeliano e ação de R) herdadas de M.

Se M é um R-módulo e $N \subseteq M$ é um submódulo de M, então define-se o R-módulo quociente, M/N, como o grupo quociente com a ação: $\cdot : R \times M/N \to M/N$ definida por $r.(m + N) = rm + N$, $\forall\, r \in R, m \in M$.

Definição 1.2.25. Um módulo satisfaz a *condição de cadeias ascendentes* (dizemos simplesmente ACC) nos submódulos se toda cadeia ascendente de submódulos deste módulo estabiliza. Neste caso, o módulo é chamado de *noetheriano*.

Um anel é *noetheriano* quando satisfaz ACC em ideais, ou seja, considerando-o como um módulo sobre si mesmo.

Proposição 1.2.26. As seguintes condições sobre um R-módulo M são equivalentes:

(i) M é noetheriano.

(ii) Toda família não vazia de submódulos de M possui um elemento maximal.

(iii) Todo submódulo de M é finitamente gerado.

Teorema 1.2.27 (da Base de Hilbert)**.** Se R é um anel noetheriano e $n \in \mathbb{N}^{\bullet}$, então o anel de polinômios $R[x_1, \ldots, x_n]$ também é noetheriano. Em particular, se $\mathbb{K}$ é um corpo, então $\mathbb{K}[x_1, \ldots, x_n]$ é noetheriano.

Lema 1.2.28 (de Nakayama)**.** Sejam R um anel, $I \subseteq R$ um ideal contido em todo ideal maximal de R e M um R-módulo finitamente gerado. Se $I.M = M$, então $M = 0$.

Considere R um anel local, cujo único ideal maximal é $\mathfrak{m}$, e M um R-módulo. Como $\mathfrak{m}$ é maximal, $R/\mathfrak{m}$ é um corpo. Como M é um R-módulo, considere o conjunto $\mathfrak{m}M = \{r.m \mid r \in \mathfrak{m}, m \in M\}$. Este conjunto $\mathfrak{m}M$ é um submódulo de M. Considere o módulo quociente $M/\mathfrak{m}M$. Os elementos de $\mathfrak{m}$ anulam $M/\mathfrak{m}M$, ou seja, $r.(m + \mathfrak{m}M) = (0 + \mathfrak{m}M))$, $\forall\, r \in \mathfrak{m}, m \in M$. Portanto $M/\mathfrak{m}M$ é naturalmente um $R/\mathfrak{m}$-espaço vetorial.

Lema 1.2.29. Se R é um anel noetheriano local e $\mathfrak{m} \subseteq R$ é seu único ideal maximal, então: $\mathfrak{m}$ é gerado como um R-módulo por $\{r_1, \ldots, r_m\}$ se, e somente se, $\mathfrak{m}/\mathfrak{m}^2$ é gerado como um $R/\mathfrak{m}$-espaço vetorial por $\{\overline{r_1}, \ldots, \overline{r_m}\}$, onde, para cada i, $\overline{r_i}$ é a imagem de r_i pelo morfismo canônico de $\mathfrak{m}$ para $\mathfrak{m}/\mathfrak{m}^2$.

Definição 1.2.30. A *dimensão de Krull* de um anel R é o supremo dos comprimentos de cadeias próprias de ideais primos $P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \ldots \subsetneq P_k \subsetneq R$.

Definição 1.2.31. Seja R um anel. Um subconjunto $S \subseteq R$ é um *conjunto multiplicativamente fechado* quando S é fechado sob multiplicação e contém e_R. Para um R-módulo M, define-se uma relação de equivalência em $M \times S$ da seguinte forma: para quaisquer $(m_1, s_1), (m_2, s_2) \in M \times S$, $(m_1, s_1) \approx (m_2, s_2)$ quando existe $t \in S$, tal que $t(s_1 m_2 - s_2 m_1) = 0$.

Considerando R como R-módulo, define-se adição e multiplicação no conjunto das classes de equivalência, $(R \times S)/\approx$, da seguinte forma: para quaisquer $(r_1, s_1), (r_2, s_2) \in R \times S$, $(r_1, s_1) + (r_2, s_2) = ((s_1 r_2 + s_2 r_1), (s_1 s_2))$ e $(r_1, s_1).(r_2, s_2) = ((r_1 r_2), (s_1 s_2))$. O anel assim definido é denotado por $S^{-1}R$ e chamado de *anel de frações*.

Considerando um R-módulo M, define-se uma estrutura de $S^{-1}R$-módulo em $(M \times S)/\approx$ da seguinte forma: para quaisquer $(r, t) \in S^{-1}R$, $(m_1, s_1), (m_2, s_2) \in M \times S$, $(m_1, s_1) + (m_2, s_2) = (s_2 m_1 + s_1 m_2, s_1 s_2)$ e $(r, t).(m_1, s_1) = (rm_1, ts_1)$. O $S^{-1}R$-módulo assim definido é denotado por $S^{-1}M$ e chamado de *módulo de frações*.

Exemplo 1.2.32.

(i) Seja D um domínio. O *corpo de frações* de D é o anel de frações $S^{-1}D$, onde $S = D^\bullet$.

(ii) Sejam R um anel e P um ideal primo de R. Pela definição de ideais primos, $R \setminus P$ é um conjunto multiplicativamente fechado. Então é possível formar o anel de frações $(R \setminus P)^{-1}R$. Esse anel de frações é denotado por R_P e é chamado de *localização de R em P*.

Proposição 1.2.33. Seja R um anel.

(i) Para todo ideal primo $P \subseteq R$, a localização R_P é um anel local cujo ideal maximal é $PR_P = \{(p, r) \in R_P \mid p \in P, r \in R \setminus P\}$.

(ii) Sejam $S \subseteq R$ um conjunto multiplicativamente fechado e $i : R \to S^{-1}R$ o morfismo de anéis definido por $i(r) = (r, e)$, $\forall\, r \in R$. Para todo morfismo de anéis $\varphi : R \to R'$, tal que $\varphi(S) \subseteq (R')^\times$, existe um único morfismo de anéis $\widetilde{\varphi} : S^{-1}R \to R'$, para o qual comuta o diagrama
$$\begin{tikzcd} R \arrow[r, "i"] \arrow[dr, "\varphi"'] & S^{-1}R \arrow[d, "\widetilde{\varphi}"] \\ & R' \end{tikzcd}$$

Definição 1.2.34. Sejam R, S dois anéis. Se R é um subanel de S, diz-se que $R \subseteq S$ é uma *extensão de anéis*.

Seja $R \subseteq S$ uma extensão de anéis. Diz-se que um elemento $s \in S$ é *inteiro sobre* R, quando existe um polinômio mônico e não nulo $f \in R[x]$, tal que $f(s) = 0$. Diz-se que a extensão $R \subseteq S$ é *inteira* quando todo $s \in S$ é inteiro sobre R.

Observe que a idéia de extensão inteira de anéis é próxima àquela de extensão algébrica (na última não se exige que os polinômios sejam mônicos). No caso de corpos, como todo elemento não nulo é inversível, a exigência de trabalhar-se com polinômios mônicos é inócua e os dois conceitos coincidem (mas a nomenclatura "inteira" não é usada neste caso).

Observe também que todo $r \in R$ é algébrico sobre R, pois o polinômio linear $f(x) = x - r \in R[x]$ é não nulo e tem r como raiz.

Em analogia com a teoria de extensões algébricas de corpos, é natural estudar o conceito de extensão inteira de anéis em termos de adjunções.

Definição 1.2.35. Sejam $R \subseteq S$ uma extensão de domínios e $\mathcal{B}$ um subconjunto de S. O anel obtido de R por adjunção de $\mathcal{B}$, denotado por $R[\mathcal{B}]$, é a intersecção de todos os subanéis de S contendo R e $\mathcal{B}$. O corpo de frações de $R[\mathcal{B}]$ é denotado por $R(\mathcal{B})$.

Quando $\mathcal{B}$ é um conjunto finito, $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$, usa-se a notação $R[\beta_1, \ldots, \beta_n]$ para $R[\mathcal{B}]$ e $R(\beta_1, \ldots, \beta_n)$ para $R(\mathcal{B})$.

Quando o anel de polinômios $R[x_1, \ldots, x_n]$ for considerado, $R(x_1, \ldots, x_n)$ denotará o seu corpo de frações.

Proposição 1.2.36. Sejam $R \subseteq S$ uma extensão de anéis e $\mathcal{B}$ um subconjunto finito de S. $\mathcal{B}$ é inteiro sobre R se, e somente se, $R[\mathcal{B}]$ for um R-módulo finitamente gerado.

Definição 1.2.37. Seja $R \subseteq S$ uma extensão de anéis.

(i) O conjunto de todos os elementos $s \in S$ que são inteiros sobre R é chamado de *fecho inteiro* de R em S.

(ii) Se R for seu próprio fecho inteiro, então ele será dito *integralmente fechado* em S.

(iii) Se $f : R \to S$ for um morfismo de anéis e S for inteiro sobre $f(R)$, então S será chamado de *R-álgebra inteira*.

Proposição 1.2.38. Sejam $R \subseteq S \subseteq A$ extensões de anéis.

(i) O fecho inteiro de R em S é um subanel de S que contém R.

(ii) Se $R \subseteq S$ e $S \subseteq A$ são inteiras, então $R \subseteq A$ é inteira.

(iii) O fecho inteiro de R em S é integralmente fechado em S.

Proposição 1.2.39. Seja $R \subseteq S$ uma extensão inteira de anéis, então:

(i) Para todo ideal $I \subseteq S$, S/I é inteiro sobre $R/(I \cap R)$.

(ii) Para todo subconjunto multiplicativamente fechado $U \subseteq R$, o anel de frações $U^{-1}S$ é inteiro sobre $U^{-1}R$.

Definição 1.2.40. Seja $\mathbb{F} \subseteq \mathbb{L}$ uma extensão de corpos. Um subconjunto $S \subseteq \mathbb{L}$ é dito *algebricamente dependente* sobre $\mathbb{F}$ se existirem $f \in \mathbb{K}[x_1, \ldots, x_m]^\bullet$ e um subconjunto finito $\{s_1, \ldots, s_m\} \subseteq S$ tais que $f(s_1, \ldots, s_m) = 0$. Caso contrário, S é dito *algebricamente independente*. Uma *base de transcendência* de $\mathbb{L}$ sobre $\mathbb{F}$ é um subconjunto $S \subseteq \mathbb{L}$ que é algebricamente independente sobre $\mathbb{F}$ e maximal no conjunto de todos os subconjuntos de $\mathbb{L}$ algebricamente independentes sobre $\mathbb{F}$. O *grau de transcendência* de $\mathbb{L}$ sobre $\mathbb{F}$ é a cardinalidade de uma base de transcendência. Diz-se que $\mathbb{L}$ é uma extensão *puramente transcendental* de $\mathbb{F}$ se existe S uma base de transcendência de $\mathbb{L}$ sobre $\mathbb{F}$, tal que $\mathbb{L} = \mathbb{F}(S)$.

Proposição 1.2.41. Sejam $\mathbb{F} \subseteq \mathbb{L}$ uma extensão de corpos. Se $S = \{s_1, \ldots, s_n\} \subseteq \mathbb{L}$ é um subconjunto finito e algebricamente independente sobre $\mathbb{F}$, então existe um isomorfismo de $\mathbb{F}$-álgebras, $\mathbb{F}(S) \xrightarrow{\simeq} \mathbb{F}(x_1, \ldots, x_n)$.

Definição 1.2.42. Seja R um anel. Um endomorfismo δ do grupo abeliano $(R, +)$ é uma *derivação* de R se satisfizer a regra de Leibniz, isto é, se $\delta(rs) = \delta(r)s + r\delta(s)$ para todo $r, s \in R$. O conjunto de todas as derivações de R será denotado por $Der(R)$.

Proposição 1.2.43. Se R é um anel e $\delta \in Der(R)$, então $\delta(u) = 0$ para todo $u \in R^\times$.

1.3 Álgebras de Hopf

Esta seção tem como objetivo expor as definições básicas da teoria de álgebras de Hopf, suas mais importantes propriedades e seus principais resultados (sem demonstrações). A principal referência para estas definições e estes resultados é [Mon].

Nessa seção álgebras não serão consideradas necessariamente comutativas, a menos de menção contrária.

Definição 1.3.1. Seja $\mathbb{K}$ um corpo. Uma $\mathbb{K}$-álgebra (associativa com unidade) é um anel $(A, +, \mu)$ munido de um morfismo de anéis $u : \mathbb{K} \to A$ satisfazendo os seguintes diagramas comutativos:

(i) Associatividade :

$$\begin{tikzcd} A \otimes_{\mathbb{K}} A \otimes_{\mathbb{K}} A \arrow[r, "\mu \otimes id"] \arrow[d, "id \otimes \mu"'] & A \otimes_{\mathbb{K}} A \arrow[d, "\mu"] \\ A \otimes_{\mathbb{K}} A \arrow[r, "\mu"] & A \end{tikzcd}$$

(ii) Unidade :

$$\begin{tikzcd} & A \otimes_{\mathbb{K}} A \arrow[dd, "\mu"] & \\ \mathbb{K} \otimes_{\mathbb{K}} A \arrow[ur, "u \otimes id"] \arrow[dr, "\simeq"'] & & A \otimes_{\mathbb{K}} \mathbb{K} \arrow[ul, "id \otimes u"'] \arrow[dl, "\simeq"] \\ & A & \end{tikzcd}$$

onde o isomorfismo entre $A \otimes_{\mathbb{K}} \mathbb{K}$ e A é dado por $a \otimes k \mapsto ka$ e o isomorfismo entre $\mathbb{K} \otimes_{\mathbb{K}} A$ e A é dado por $k \otimes a \mapsto ka$, $\forall\ k \in \mathbb{K},\ a \in A$.

A álgebra A é dita *comutativa* se o seguinte diagrama for comutativo

(iii) Comutatividade :

$$\begin{tikzcd} A \otimes_{\mathbb{K}} A \arrow[rr, "P"] \arrow[dr, "\mu"'] & & A \otimes_{\mathbb{K}} A \arrow[dl, "\mu"] \\ & A & \end{tikzcd}$$

onde P é a permutação $P(a \otimes a') = a' \otimes a$.

Esta definição de álgebra é equivalente àquela feita em 1.2.18. O motivo para esta definição é que o ponto de vista de diagramas comutativos ajuda a definir álgebras de Hopf.

Exemplo 1.3.2. O produto tensorial de duas álgebras (A, μ_A, u_A) e (B, μ_B, u_B) é também uma álgebra com a multiplicação definida por $\mu((a \otimes b), (a' \otimes b')) = \mu_A(a, a') \otimes \mu_B(b, b')$, para quaisquer $a, a' \in A$ e $b, b' \in B$.

Nessa linguagem, o conceito de morfismo de álgebra é reescrito como:

Definição 1.3.3. Uma função $\mathbb{K}$-linear $f : A \to B$ entre duas $\mathbb{K}$-álgebras é um *morfismo de álgebras* se os seguintes diagramas são comutativos:

$$
\begin{tikzcd}
A \otimes_{\mathbb{K}} A \arrow[r, "f\otimes f"] \arrow[d, "\mu_A"'] & B \otimes_{\mathbb{K}} B \arrow[d, "\mu_B"] \\
A \arrow[r, "f"'] & B
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[rr, "f"] & & B \\
& \mathbb{K} \arrow[ul, "u_A"] \arrow[ur, "u_B"'] &
\end{tikzcd}
$$

Em dualidade ao conceito de álgebra está o conceito de coálgebra.

Definição 1.3.4. Sejam $\mathbb{K}$ um corpo e C um espaço vetorial sobre $\mathbb{K}$. Diz-se que C é uma *coálgebra* sobre $\mathbb{K}$ quando existirem funções $\mathbb{K}$-lineares, $\Delta : C \to C \otimes_{\mathbb{K}} C$ e $\varepsilon : C \to \mathbb{K}$, chamadas respectivamente de *comultiplicação* e *counidade*, satisfazendo os seguintes diagramas comutativos

(i) Coassociatividade :

$$
\begin{tikzcd}
C \otimes_{\mathbb{K}} C \otimes_{\mathbb{K}} C & C \otimes_{\mathbb{K}} C \arrow[l, "\Delta\otimes id"'] \\
C \otimes_{\mathbb{K}} C \arrow[u, "id\otimes\Delta"] & C \arrow[l, "\Delta"] \arrow[u, "\Delta"']
\end{tikzcd}
$$

(ii) Counidade :

$$
\begin{tikzcd}
& C \otimes_{\mathbb{K}} C \arrow[dl, "\varepsilon\otimes id"'] \arrow[dr, "id\otimes\varepsilon"] & \\
\mathbb{K} \otimes_{\mathbb{K}} C & & C \otimes_{\mathbb{K}} \mathbb{K} \\
& C \arrow[ul, "\simeq"] \arrow[ur, "\simeq"'] \arrow[uu, "\Delta"] &
\end{tikzcd}
$$

onde o isomorfismo entre C e $C \otimes_{\mathbb{K}} \mathbb{K}$ é dado por $c \mapsto c \otimes 1$ e o isomorfismo entre C e $\mathbb{K} \otimes_{\mathbb{K}} C$ é dado por $c \mapsto 1 \otimes c$, $\forall\, c \in C$.

A coálgebra C é dita *cocomutativa*, quando o seguinte diagrama for comutativo

(iii) Cocomutatividade :

$$
\begin{tikzcd}
C \otimes_{\mathbb{K}} C & & C \otimes_{\mathbb{K}} C \arrow[ll, "P"'] \\
& C \arrow[ul, "\Delta"] \arrow[ur, "\Delta"'] &
\end{tikzcd}
$$

Devido a coassociatividade, $(id\otimes\Delta)\circ\Delta = (\Delta\otimes id)\circ\Delta$ como morfismos de C para $C\otimes C\otimes C$. Por isso, é possível definir para todo $c \in C$, $\Delta^2(c) = (id \otimes \Delta) \circ \Delta(c) = (\Delta \otimes id) \circ \Delta(c)$. Analogamente, é possível definir $\Delta^n(c) \in C^{\otimes n+1}$ para todo $n \in \mathbb{N}$.

Definição 1.3.5. Sejam C e D duas coálgebras sobre o corpo $\mathbb{K}$. Um *morfismo de coálgebras* é uma função $\mathbb{K}$-linear $f : C \to D$, que faz os seguintes diagramas comutarem:

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[d, "\Delta_C"'] & D \arrow[d, "\Delta_D"] \\ C \otimes_{\mathbb{K}} C \arrow[r, "f\otimes f"'] & D \otimes_{\mathbb{K}} D \end{tikzcd} \qquad \begin{tikzcd} C \arrow[rr, "f"] \arrow[dr, "\varepsilon_C"'] & & D \arrow[dl, "\varepsilon_D"] \\ & \mathbb{K} & \end{tikzcd}$$

Exemplo 1.3.6.

(i) O próprio corpo $\mathbb{K}$ é uma coálgebra com $\varepsilon(k) = k$ e $\Delta(k) = k \otimes k$, para todo $k \in \mathbb{K}$. Se (C, Δ, ε) é uma coálgebra, então $\varepsilon : C \to \mathbb{K}$ é um morfismo de coálgebras.

(ii) O produto tensorial de duas coálgebras C e D tem uma estrutura de coálgebra dada por $\varepsilon = \varepsilon_C \otimes \varepsilon_D$ e $\Delta = (id_C \otimes P_{C,D} \otimes id_D) \circ (\Delta_C \otimes \Delta_D)$, onde $P_{C,D}(x, y) = (y, x), \forall\, x \in C,\ y \in D$.

(iii) O anel de polinômios $\mathbb{K}[x]$ é uma coálgebra com $\Delta(1) = 1 \otimes 1$, $\varepsilon(1) = 1$ e $\Delta(x^n) = (1 \otimes x + x \otimes 1)^n$ e $\varepsilon(x^n) = 0$, se $n \in \mathbb{N}^\bullet$.

(iv) O anel de polinômios de Laurent $\mathbb{K}[x, x^{-1}]$ é uma coálgebra com $\Delta(x^n) = x^n \otimes x^n$ e $\varepsilon(x^n) = 1$, para todo $n \in \mathbb{Z}$.

Proposição 1.3.7. Seja $(H, \mu, u, \Delta, \varepsilon)$ um espaço vetorial sobre um corpo $\mathbb{K}$ munido com estruturas de álgebra (H, μ, u) e coálgebra (H, Δ, ε). As afirmações abaixo são equivalentes:

(i) As funções μ e u são morfismos de coálgebras.

(ii) As funções Δ e ε são morfismos de álgebras.

Agora, a próxima definição se torna natural:

Definição 1.3.8. Uma *biálgebra* é um $\mathbb{K}$-espaço vetorial H que munido com estruturas de álgebra (H, μ, u) e coálgebra (H, Δ, ε) satisfaz uma das condições da proposição acima. Um *morfismo de biálgebras* é uma função entre biálgebras que é simultaneamente morfismo de álgebras e coálgebras.

Definição 1.3.9. Seja $(H, \mu, u, \Delta, \varepsilon)$ uma biálgebra. Uma função $\mathbb{K}$-linear $S : H \to H$ é chamada de *antípoda* quando faz os seguintes diagramas comutarem:

$$\begin{tikzcd} H \otimes H \arrow[r, "S\otimes id"] & H \otimes H \arrow[d, "\mu"] \\ H \arrow[u, "\Delta"] \arrow[r, "u\circ\varepsilon"] & H \end{tikzcd} \qquad \begin{tikzcd} H \otimes H \arrow[r, "id\otimes S"] & H \otimes H \arrow[d, "\mu"] \\ H \arrow[u, "\Delta"] \arrow[r, "u\circ\varepsilon"] & H \end{tikzcd}$$

Uma *álgebra de Hopf* é uma biálgebra munida de uma função antípoda.

O seguinte teorema coleta algumas propriedades da antípoda.

Teorema 1.3.10. Seja $(H, \mu, u, \Delta, \varepsilon)$ uma biálgebra.

(*i*) Se H possuir uma função antípoda, então ela é única.

(*ii*) A antípoda é um anti-homomorfismo de biálgebras, ou seja, $S \circ \mu = \mu^{\mathrm{op}} \circ (S \otimes S)$, $S(1) = 1$, $(S \otimes S) \circ \Delta = \Delta^{\mathrm{op}} \circ S$ e $\varepsilon \circ S = \varepsilon$, onde $\mu^{\mathrm{op}} = \mu \circ P$ e $\Delta^{op} = P \circ \Delta$.

Definição 1.3.11. Sejam $\mathbb{K}$ um corpo e $(H, \mu, u, \Delta, \varepsilon, S)$ uma $\mathbb{K}$-álgebra de Hopf. Defina o *ideal de aumento* de H como o núcleo da counidade ε.

Proposição 1.3.12. Se (C, Δ, ε) é uma coálgebra, então o espaço vetorial dual $C^* = Hom_{Mod_{\mathbb{K}}}(C, \mathbb{K})$ é uma álgebra com multiplicação dada por Δ^*, onde $\Delta^*(\varphi, \psi) = (\varphi \otimes \psi) \circ \Delta$ e com unidade dada por ε^*, onde $\varepsilon^*(\varphi) = \varphi \circ \varepsilon$, $\forall\ \varphi, \psi \in Hom_{Mod_{\mathbb{K}}}(C, \mathbb{K})$.

Na proposição acima considera-se $C^* \otimes C^*$ como uma subálgebra de $(C \otimes C)^*$ com inclusão dada por $\iota : C^* \otimes C^* \to (C \otimes C)^*$; $\iota(\varphi \otimes \psi)(c_1 \otimes c_2) = \varphi(c_1)\psi(c_2)$, $\forall\ \varphi, \psi \in C^*,\ c_1 \otimes c_2 \in C \otimes C$. No entanto uma construção análoga para álgebras nem sempre é possível. De fato, nem sempre o dual de uma álgebra A é uma coálgebra com as operações duais análogas, pois uma inclusão de $(A \otimes A)^*$ em $A^* \otimes A^*$ nem sempre existe. No caso em que a dimensão de A é finita, uma inclusão $\iota : (A \otimes A)^* \to A^* \otimes A^*$ sempre existe, mas no caso de dimensão infinita, não. Para resolver este problema, faz-se a seguinte definição:

Definição 1.3.13. Seja A uma $\mathbb{K}$-álgebra. Define-se o *dual finito* de A como o conjunto $A^\circ = \{f \in A^* \mid f(I) = 0,\ \text{para algum ideal } I \subseteq A,\ \text{tal que } \dim(A/I) < \infty\}$.

Proposição 1.3.14. Se (A, μ, u) é uma $\mathbb{K}$-álgebra, então A° é uma coálgebra com a comultiplicação definida por $\mu^*(f) = f \circ \mu$ e a counidade definida por $u^*(f) = f \circ u$, $\forall\ f \in A^\circ$.

1.4 Álgebras de Lie

Esta seção contéem uma breve exposição dos conceitos básicos de álgebras de Lie. Uma referência para as definições e resultados expostos (assim como para as demonstrações omitidas) é [Jac].

Definição 1.4.1. Seja $\mathbb{K}$ um corpo. Uma *álgebra de Lie* sobre $\mathbb{K}$ é um $\mathbb{K}$-espaço vetorial $\mathfrak{g}$ munido de uma função bilinear, $[\ ,\ ] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$, anticomutativa e que satisfaz a identidade de Jacobi, ou seja:

(*i*) $[\mathsf{x}, \mathsf{x}] = 0$, para todo $\mathsf{x} \in \mathfrak{g}$;

(*ii*) $[[\mathsf{x}, \mathsf{y}], \mathsf{z}] + [[\mathsf{z}, \mathsf{x}], \mathsf{y}] + [[\mathsf{y}, \mathsf{z}], \mathsf{x}] = 0$, para quaisquer $\mathsf{x}, \mathsf{y}, \mathsf{z} \in \mathfrak{g}$.

Essa transformação $[\ ,\ ]$ é chamada de *colchete de Lie*.

Uma *subálgebra de Lie* da álgebra de Lie $\mathfrak{g}$ é um $\mathbb{K}$-subespaço vetorial de $\mathfrak{g}$ que, munido do mesmo colchete de Lie, é uma álgebra de Lie.

Observação 1.4.2.

(*i*) Quando o corpo $\mathbb{K}$ é de característica diferente de 2, a condição (*i*) da definição acima é equivalente a $[\mathsf{x}, \mathsf{y}] = -[\mathsf{y}, \mathsf{x}]$, $\forall\, \mathsf{x}, \mathsf{y} \in \mathfrak{g}$. Por iso tal condição é chamada de anticomutatividade.

(*ii*) A identidade de Jacobi pode ser reescrita como $[\mathsf{x}, [\mathsf{y}, \mathsf{z}]] = [[\mathsf{x}, \mathsf{y}], \mathsf{z}] + [\mathsf{y}, [\mathsf{x}, \mathsf{z}]]$.

Exemplo 1.4.3. Alguns exemplos importantes de álgebras de Lie:

(i) Todo espaço vetorial V munido do colchete trivial, ou seja, $[v, w] = 0$, $\forall\ v, w \in V$, é uma álgebra de Lie. Tais álgebras de Lie, cujo colchete é trivial, são chamadas de *abelianas*.

(ii) O conjunto das matrizes de ordem n, denotado por $\mathfrak{gl}_n$, com o colchete dado por $[A, B] = AB - BA$, para quaisquer $A, B \in \mathfrak{gl}_n$, forma uma álgebra de Lie.

(iii) $\mathfrak{sl}_n$ é a subálgebra de $\mathfrak{gl}_n$ formada pelas matrizes de traço zero.

(iv) $\mathfrak{sp}_{2n}$ é a subálgebra de $\mathfrak{gl}_{2n}$ formada pelas matrizes que preservam uma forma bilinear antissimétrica e não degenerada.

(v) $\mathfrak{so}_n$ é a subálgebra de $\mathfrak{gl}_n$ formada pelas matrizes que preservam uma forma bilinear simétrica e não degenerada.

Os exemplos acima são as chamadas *álgebras clássicas*. As álgebras clássicas são casos particulares da seguinte construção geral:

(vi) Se A é uma $\mathbb{K}$-álgebra associativa, então $A^{(-)}$ é uma álgebra de Lie, cujo espaço vetorial subjacente é o próprio A e o colchete é dado pelo *comutador* em A, ou seja, $[a, b] = ab - ba$, $\forall\ a, b \in A$. Em particular, se V é um $\mathbb{K}$-espaço vetorial $\mathfrak{gl}(V)$, o conjunto dos endomorfismos de V, é uma álgebra de Lie.

(vii) $\mathfrak{t}_n(\mathbb{K})$ é a subálgebra de $\mathfrak{gl}_n(\mathbb{K})$ formada pelas matrizes triangulares superiores.

$(viii)$ $\mathfrak{n}_k(\mathbb{K})$ é a subálgebra de $\mathfrak{gl}_k(\mathbb{K})$ formada pelas matrizes estritamente triangulares superiores.

(ix) $\mathfrak{d}_n(\mathbb{K})$ é a subálgebra de $\mathfrak{gl}_n(\mathbb{K})$ formada pelas matrizes diagonais.

Considere $\mathfrak{g}$ uma álgebra de Lie. Munida do colchete de Lie, $\mathfrak{g}$ não é uma álgebra no sentido da definição 1.2.18, pois $\mathfrak{g}$ não é um anel associativo nem comutativo com unidade. No entanto, considerando-se o colchete de Lie como uma multiplicação no espaço vetorial $\mathfrak{g}$, obtem-se um "anel" onde a anticomutatividade substitui a comutatividade e a identidade de Jacobi substitui a associatividade. Nesse sentido a álgebra de Lie é uma álgebra (anticomutativa, não associativa e sem unidade) e as definições a seguir se tornam naturais.

Definição 1.4.4. Sejam $\mathfrak{g}$ e $\mathfrak{h}$ duas álgebras de Lie sobre o corpo $\mathbb{K}$. Uma transformação $\mathbb{K}$-linear $\varphi : \mathfrak{g} \to \mathfrak{h}$ é um *morfismo* de álgebras de Lie quando $\varphi([\mathsf{x}, \mathsf{y}]) = [\varphi(\mathsf{x}), \varphi(\mathsf{y})]$ para quaisquer $\mathsf{x}, \mathsf{y} \in \mathfrak{g}$.

Um subespaço vetorial $I \subseteq \mathfrak{g}$ é um *ideal* quando $[i, \mathsf{x}] \in I$ para quaisquer $i \in I$ e $\mathsf{x} \in \mathfrak{g}$. Nesse caso, define-se a *álgebra de Lie quociente* de $\mathfrak{g}$ por I como o espaço vetorial quociente $\mathfrak{g}/I$, com o colchete de Lie definido por : $[\mathsf{x} + I, \mathsf{y} + I] = [\mathsf{x}, \mathsf{y}] + I$, para quaisquer $\mathsf{x}, \mathsf{y} \in \mathfrak{g}$.

Exemplo 1.4.5. Considere a álgebra de Lie $\mathfrak{g}$ e um elemento $\mathsf{x} \in \mathfrak{g}$. Como o colchete é uma função bilinear em $\mathfrak{g}$, fixando-se a primeira entrada, induz-se uma transformação linear em $\mathfrak{g}$ definida por $[\mathsf{x}, \cdot] : \mathfrak{g} \to \mathfrak{g}$, onde $[\mathsf{x}, \cdot] : \mathsf{y} \mapsto [\mathsf{x}, \mathsf{y}]$, $\forall\ \mathsf{y} \in \mathfrak{g}$. Essa transformação linear, chamada de *adjunta*, é denotada por $ad(\mathsf{x}) : \mathfrak{g} \to \mathfrak{g}$ e é uma derivação da álgebra de Lie devido à observação 1.4.2 (ii).

Definição 1.4.6. Seja $\varphi : \mathfrak{g} \to \mathfrak{h}$ um morfismo entre álgebras de Lie.

(*i*) O *núcleo de* φ é o conjunto $\ker\varphi = \{\mathsf{x} \in \mathfrak{g} \mid \varphi(\mathsf{x}) = 0\}$.

(*ii*) A *imagem de* φ é o conjunto $im(\varphi) = \{\mathsf{y} \in \mathfrak{h} \mid \exists\, \mathsf{x} \in \mathfrak{g}$, tal que $\varphi(\mathsf{x}) = \mathsf{y}\}$.

Proposição 1.4.7. Seja $\varphi : \mathfrak{g} \to \mathfrak{h}$ um morfismo de álgebras de Lie, então:

(*i*) $\ker(\varphi)$ é um ideal de $\mathfrak{g}$;

(*ii*) $\mathfrak{g}/\ker(\varphi) \simeq im(\varphi)$.

Definição 1.4.8. Seja $\mathfrak{g}$ uma álgebra de Lie. O *centro* de $\mathfrak{g}$ é definido como o conjunto $Z(\mathfrak{g}) = \{\mathsf{x} \in \mathfrak{g} \mid [\mathsf{x}, \mathsf{y}] = 0,\ \forall\ \mathsf{y} \in \mathfrak{g}\}$. O centralizador de um subconjunto $X \subseteq \mathfrak{g}$ é definido como $C_{\mathfrak{g}}(X) = \{\mathsf{g} \in \mathfrak{g} \mid [\mathsf{g}, x] = 0,\ \forall\ x \in X\}$. O normalizador de um subespaço $V \subseteq \mathfrak{g}$ é definido como $N_{\mathfrak{g}}(V) = \{\mathsf{g} \in \mathfrak{g} \mid [\mathsf{g}, v] \in V,\ \forall\ v \in V\}$.

Proposição 1.4.9. Seguindo a notação da definição acima:

(*i*) O centralizador e o normalizador são subálgebras de $\mathfrak{g}$.

(*ii*) $C_{\mathfrak{g}}(\mathfrak{g}) = Z(\mathfrak{g})$.

(*iii*) O centro é um ideal.

Definição 1.4.10. Seja $\mathfrak{g}$ uma álgebra de Lie sobre um corpo $\mathbb{K}$. Uma *representação* de $\mathfrak{g}$ em um $\mathbb{K}$-espaço vetorial V é um morfismo de álgebras de Lie $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$. A dimensão de V é chamada de *dimensão* da representação ρ. Se ρ for injetora, então a representação é dita *fiel*.

Em geral, uma representação será denotada por (V, ρ) ou simplesmente V, apesar dela depender do morfismo ρ.

Exemplo 1.4.11.

(*i*) A adjunta (definida no exemplo 1.4.5) é uma representação da álgebra de Lie nela mesma. Ou seja, para toda álgebra de Lie $\mathfrak{g}$, $ad : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ é uma representação.

(*ii*) Para toda subálgebra de Lie $\mathfrak{g}$ da álgebra de Lie $\mathfrak{gl}_n$, existe um morfismo injetor de álgebras de Lie de $\mathfrak{g}$ em $\mathfrak{gl}_n$. Esse morfismo é uma representação que será denotada por $\rho_0 : \mathfrak{g} \to \mathfrak{gl}_n$.

Definição 1.4.12. Seja $\mathfrak{g}$ uma álgebra de Lie. Considere os ideais $\mathfrak{g}^{(k)}$ de $\mathfrak{g}$ definidos por $\mathfrak{g}^{(0)} = \mathfrak{g}$ e $\mathfrak{g}^{(k+1)} = [\mathfrak{g}^{(k)}, \mathfrak{g}^{(k)}]$ para todo $k \in \mathbb{N}$. Por construção, $\mathfrak{g}^{(k)} \supseteq \mathfrak{g}^{(k+1)}$, $\forall\ k \in \mathbb{N}$. Portanto os ideais $\mathfrak{g}^{(k)}$ formam uma cadeia descendente, chamada de *série derivada* de $\mathfrak{g}$. A álgebra de Lie $\mathfrak{g}$ é chamada *solúvel* quando $\mathfrak{g}^{(k)} = 0$ para algum $k \in \mathbb{N}$.

Agora, considere os ideais $\mathfrak{g}^k$ de $\mathfrak{g}$ definidos por $\mathfrak{g}^1 = \mathfrak{g}$ e $\mathfrak{g}^{k+1} = [\mathfrak{g}, \mathfrak{g}^k]$ para todo $k \in \mathbb{N}^\bullet$. Por construção, $\mathfrak{g}^k \supseteq \mathfrak{g}^{k+1}$, $\forall\ k \in \mathbb{N}^\bullet$. Portanto os ideais $\mathfrak{g}^k$ também formam uma cadeia descendente de ideais, chamada de *série central descendente* de $\mathfrak{g}$. A álgebra de Lie $\mathfrak{g}$ é chamada *nilpotente* quando $\mathfrak{g}^k = 0$ para algum $k \in \mathbb{N}^\bullet$.

Proposição 1.4.13.

(*i*) Toda álgebra de Lie abeliana é solúvel e nilpotente.

(*ii*) Toda álgebra de Lie nilpotente é solúvel.

(*iii*) Para toda álgebra de Lie de dimensão finita e nilpotente existe um morfismo injetor de álgebras de Lie para a álgebra de Lie de matrizes estritamente triangulares superiores.

(*iv*) Para toda álgebra de Lie de dimensão finita e solúvel sobre um corpo de característica zero existe um morfismo injetor de álgebras de Lie para a álgebra de Lie de matrizes triangulares superiores.

O item (*iii*) da proposição acima é corolário do Teorema de Engel, enquanto o item (*iv*) é corolário do Teorema de Lie.

Definição 1.4.14. Seja $\mathfrak{g}$ uma álgebra de Lie. Define-se $U(\mathfrak{g})$, a *álgebra universal envelopante* da álgebra de Lie $\mathfrak{g}$ como o quociente da álgebra tensorial de $\mathfrak{g}$ pelo ideal gerado por $\{(\mathsf{x} \otimes \mathsf{y} - \mathsf{y} \otimes \mathsf{x} - [\mathsf{x}, \mathsf{y}]) \mid \mathsf{x}, \mathsf{y} \in \mathfrak{g}\}$.

Teorema 1.4.15 (Poincaré-Birkhoff-Witt)**.** Sejam $\{\mathsf{x}_i \mid i \in I\}$ uma base ordenada para a álgebra de Lie $\mathfrak{g}$ e $\pi : T(\mathfrak{g}) \to U(\mathfrak{g})$ a projeção canônica da álgebra tensorial de $\mathfrak{g}$ sobre a universal envelopante. Então o conjunto $\{\mathsf{x}_{i_1} \ldots \mathsf{x}_{i_m} \mid m \in \mathbb{N}, i_1 \leq \ldots \leq i_m\}$, onde $\mathsf{x}_{i_1} \ldots \mathsf{x}_{i_m} = \pi(\mathsf{x}_{i_1} \otimes \ldots \otimes \mathsf{x}_{i_m})$, é uma base para $U(\mathfrak{g})$.

Observação 1.4.16. Usando o teorema acima, existe uma transformação linear injetora $i : \mathfrak{g} \hookrightarrow U(\mathfrak{g})$, tal que $i([\mathsf{x}, \mathsf{y}]) = i(\mathsf{x})i(\mathsf{y}) - i(\mathsf{y})i(\mathsf{x})$. Para toda álgebra associativa A e toda transformação linear $j : \mathfrak{g} \to A$, tal que $j([\mathsf{x}, \mathsf{y}]) = j(\mathsf{x})j(\mathsf{y}) - j(\mathsf{y})j(\mathsf{x})$, existe um único morfismo de álgebras associativas $\varphi : U(\mathfrak{g}) \to A$ que torna o seguinte diagrama comutativo:

$$\begin{tikzcd} \mathfrak{g} \arrow[r, "i"] \arrow[dr, "j"'] & U(\mathfrak{g}) \arrow[d, "\varphi"] \\ & A \end{tikzcd}$$

Observação 1.4.17 (filtração da álgebra universal)**.** Considere a seguinte filtração da álgebra tensorial T de $\mathfrak{g}$: $T_d = \bigoplus_{k \leq d} \mathfrak{g}^{\otimes k}$. Então, a partir do teorema 1.4.15, define-se uma filtração para $U(\mathfrak{g})$ como o quociente da filtração da álgebra tensorial, explicitamente, para todo $d \in \mathbb{N}$, $U_d = T_d / I_d$, onde o ideal $I_d = T_d \cap \langle \mathsf{x} \otimes \mathsf{y} - \mathsf{y} \otimes \mathsf{x} - [\mathsf{x}, \mathsf{y}] \mid \mathsf{x}, \mathsf{y} \in \mathfrak{g} \rangle$.

Como definido acima, a álgebra universal envelopante de uma álgebra de Lie é uma álgebra associativa. Além disso, ela é munida de uma estrutura de álgebra de Hopf. Explicitamente, essa estrutura é a seguinte.

Defina a comultiplicação, $\Delta : U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes U(\mathfrak{g})$ da seguinte forma: para todo $\mathsf{x} \in \mathfrak{g}$, $\Delta_U(\mathsf{x}) = 1 \otimes \mathsf{x} + \mathsf{x} \otimes 1$.

Defina a counidade, $\varepsilon : U(\mathfrak{g}) \to \mathbb{K}$, tal que, para cada $\mathsf{x} \in \mathfrak{g}$, $\varepsilon(\mathsf{x}) = 0$.

Para completar a estrutura de álgebra de Hopf, defina a antípoda $S : U(\mathfrak{g}) \to U(\mathfrak{g})$ da seguinte forma $S(\mathsf{x}) = -\mathsf{x}$, para cada $\mathsf{x} \in \mathfrak{g}$.

Não é difícil verificar que as funções Δ, ε e S podem ser estendidas de maneira única de modo que sejam homomorfismos de álgebras (ou anti-homomorfismo no caso da antípoda). Assim elas de fato definem uma estrutura de álgebra de Hopf em $U(\mathfrak{g})$.

1.5 Teoria de Categorias

O objetivo desta seção é expor as definições, os exemplos e os resultados (sem demonstração) básicos da teoria de categorias. As referências para tal tema são [Mac] e [Ana].

Definição 1.5.1. Uma *categoria* $\mathcal{C}$ consiste de:

(i) Um conjunto de *objetos*, denotada por $Obj(\mathcal{C})$.

(ii) Um conjunto de *morfismos*, denotada por $Mor(\mathcal{C})$. A coleção de morfismos da categoria $\mathcal{C}$ é a união dos conjuntos de *morfismos entre objetos*, $Mor_{\mathcal{C}}(x, y)$, $x, y \in Obj(\mathcal{C})$.

(iii) Para quaisquer objetos $x, y, z \in Obj(C)$, existe uma função chamada de *composição de morfismos* que será denotada por $\circ : Mor_{\mathcal{C}}(y, z) \times Mor_{\mathcal{C}}(x, y) \to Mor_{\mathcal{C}}(x, z)$, onde $\circ(\beta, \alpha) = \beta \circ \alpha$ para quaisquer morfismos $\alpha \in Mor_{\mathcal{C}}(x, y)$ e $\beta \in Mor_{\mathcal{C}}(y, z)$. Essa composição satisfaz as seguintes propriedades:

(a) Associatividade: $(\gamma \circ \beta) \circ \alpha = \gamma \circ (\beta \circ \alpha)$ para quaisquer morfismos $\alpha \in Mor_{\mathcal{C}}(x, y)$, $\beta \in Mor_{\mathcal{C}}(y, z)$, $\gamma \in Mor_{\mathcal{C}}(z, w)$ e objetos x, y, z e $w \in Obj(\mathcal{C})$.

(b) Para qualquer objeto $x \in Obj(\mathcal{C})$, existe um morfismo $id_x \in Mor_{\mathcal{C}}(x, x)$, tal que $id_x \circ \alpha = \alpha$ para todo objeto $y \in Obj(\mathcal{C})$ e para todo morfismo $\alpha \in Mor_{\mathcal{C}}(y, x)$ e $\alpha \circ id_x = \alpha$ para todo objeto $y \in Obj(\mathcal{C})$ e para todo morfismo $\alpha \in Mor_{\mathcal{C}}(x, y)$.

Os morfismos são usualmente chamados de setas e denotados por setas. Quando não gerar confusão, serão omitidos o símbolo $\circ$ de composição, assim como o subescrito $_{\mathcal{C}}$ relativo à categoria em que os morfismos são considerados. Usualmente os conjuntos Mor são denotados por Hom.

Exemplo 1.5.2.

(1) Considere a coleção dos conjuntos como a coleção de objetos e a coleção de funções entre conjuntos como a coleção de morfismos, munido de composição usual de funções. Isso forma uma categoria, chamada de *categoria de conjuntos* e denotada por **Sets**[1]

(2) Categorias algébricas.

(i) A *categoria de grupos* é a categoria de cujo conjunto de objetos consiste de todos os grupos e o conjunto de morfismos consiste de homomorfismos entre grupos. Essa categoria é denotada por **Grp**.

(ii) A *categoria de anéis* é a categoria de cujo conjunto de objetos consiste de todos os anéis e o conjunto de morfismos consiste de morfismos entre anéis. Essa categoria é denotada por **Rng**.

(iii) Dado um anel R, a *categoria de R-módulos* é a categoria cujo conjunto de objetos consiste de todos os R-módulos e o conjunto de morfismos consiste de morfismos de R-módulos. Essa categoria é denotada por $\mathbf{Mod}_R$. Em particular, quando R é um corpo, $\mathbf{Mod}_R$ é a categoria de R-espaços vetoriais.

[1] Não nos preocuparemos muito com os fundamentos da matemática. De fato, para evitar o paradoxo de Russel, deve-se considerar somente os conjuntos de cardinalidade limitada. Outra maneira seria considerar dois conjuntos, chamados de universos, e considerar somente as classes pequenas.

(iv) Dado um anel R, a *categoria de R-álgebras* é a categoria cujo conjunto de objetos consiste de todas as R-álgebras e o conjunto de morfismos consiste de morfismos de R-álgebras. Essa categoria é denotada por $\mathbf{Alg}_R$.

(3) Categorias topológicas.

(i) A categoria cujos objetos são espaços topológicos e os morfismos são funções contínuas entre espaços topológicos é chamada de *categoria Top*. Essa categoria é denotada por **Top**.

(ii) A categoria cujos objetos são classes de equivalência de espaços topológicos a menos de homotopia e os morfismos são classes de equivalência de funções contínuas a menos de equivalência homotópica é denotada por $\mathbf{Top}_h$.

(iii) A categoria cujos objetos são classes de equivalência de pares (X, x_0), onde $X \in \mathbf{Top}_h$, $x_0 \in X$ é um ponto-base e os morfismos são classes de equivalência de funções contínuas entre espaços topológicos, que preservam ponto-base. Duas funções contínuas são ditas equivalentes se existe uma equivalência homotópica entre elas que preserva o ponto-base. Essa categoria é denotada por $\mathbf{Top}_h^0$.

Definição 1.5.3. Sejam $\mathcal{C}$ uma categoria, $x, y \in Obj(\mathcal{C})$ e $\alpha \in Hom_{\mathcal{C}}(x, y)$. Diz-se que α é uma *equivalência* ou *isomorfismo* entre x e y quando existe um morfismo $\beta \in Hom_{\mathcal{C}}(y, x)$, tal que $\alpha \circ \beta = id_y$ e $\beta \circ \alpha = id_x$. Nesse caso, β é chamado de *inverso* de α.

Definição 1.5.4. Sejam $\mathcal{C}$ e $\mathcal{C}'$ duas categorias. Um *funtor covariante* $F : \mathcal{C} \to \mathcal{C}'$ consiste de um par de funções denotadas pelo mesmo símbolo $F : Obj(\mathcal{C}) \to Obj(\mathcal{C}')$ e $F : Mor(\mathcal{C}) \to Mor(\mathcal{C}')$, que satisfazem:

(i) Para todo $x \in Obj(\mathcal{C})$, $F(id_x) = id_{F(x)}$;

(ii) Para quaisquer $x, y, z \in Obj(\mathcal{C})$, $\alpha \in Hom(x, y)$ e $\beta \in Hom(y, z)$, $F(\beta \circ \alpha) = F(\beta) \circ F(\alpha)$.

Quando $F : \mathcal{C} \to \mathcal{C}'$ satisfaz (i) e

(ii′) Para quaisquer $x, y, z \in Obj(\mathcal{C})$, $\alpha \in Hom(x, y)$ e $\beta \in Hom(y, z)$, $F(\beta \circ \alpha) = F(\alpha) \circ F(\beta)$, F é chamado de *funtor contravariante*.

Exemplo 1.5.5.

(i) É possível formar, agora, a categoria de Categorias, cujos objetos são categorias e cujos morfismos são funtores. Essa categoria é denotada por **Cat**.

(ii) A função $\pi_1 : \mathbf{Top_h^0} \to \mathbf{Grp}$ que associa a cada (X, x_0), o grupo fundamental $\pi_1(X, x_0)$ é um funtor covariante.

(iii) Sejam $\mathcal{C}$ uma categoria e c um objeto de $\mathcal{C}$. A função $Hom(c, \cdot) : \mathcal{C} \to \mathbf{Sets}$ definida por $Hom(c, \cdot)(x) = Hom(c, x)$, para todo $x \in Obj(\mathcal{C})$, é um funtor covariante. Analogamente, podemos definir um funtor contravariante $Hom(\cdot, c)$. Qualquer funtor isomorfo a um funtor da forma $Hom(c, \cdot)$ ou $Hom(\cdot, c)$ é chamado de *funtor representável*.

(iv) O *funtor de esquecimento* é um funtor que "esquece" alguma estrutura da categoria. Por exemplo, o funtor $E : \mathbf{Grp} \to \mathbf{Sets}$ que associa a cada grupo o respectivo conjunto subjacente é um funtor de esquecimento.

Definição 1.5.6. Sejam $F, F' : \mathcal{C} \to \mathcal{C}'$ dois funtores entre categorias. Uma *transformação natural* $\eta : F \to F'$ é uma coleção de morfismos $\eta_c : F(c) \to F'(c)$, $c \in Obj(\mathcal{C})$, tal que, para todo $\alpha \in Hom_{\mathcal{C}}(x, y)$, $F'(\alpha) \circ \eta_x = \eta_y \circ F(\alpha)$, ou seja, o seguinte diagrama é comutativo:

$$\begin{tikzcd} F(x) \arrow[r, "F(\alpha)"] \arrow[d, "\eta_x"'] & F(y) \arrow[d, "\eta_y"] \\ F'(x) \arrow[r, "F'(\alpha)"'] & F'(y) \end{tikzcd}$$

Definição 1.5.7. Seja $\mathcal{C}$ uma categoria. Um objeto $c \in Obj(\mathcal{C})$ é um *objeto final* da categoria $\mathcal{C}$ quando existe uma única seta $\alpha \in Hom(x, c)$ para todo objeto $x \in Obj(\mathcal{C})$. Um objeto $c \in Obj(\mathcal{C})$ é um *objeto inicial* da categoria $\mathcal{C}$ quando existe uma única seta $\alpha \in Hom_{\mathcal{C}}(c, x)$ para todo objeto $x \in Obj(\mathcal{C})$.

Observe que, quando existem, os objetos iniciais e finais em uma categoria são únicos a menos de isomorfismos. De fato, se existem dois objetos iniciais distintos $c_1, c_2 \in Obj(\mathcal{C})$, então existem únicas setas $c_1 \xrightarrow{\alpha_{12}} c_2$ e $c_2 \xrightarrow{\alpha_{21}} c_1$. Além disso, também existem setas id_{c_1} e id_{c_2}. Pela unicidade de α_{12} e α_{21}, $\alpha_{21} \circ \alpha_{12} = id_{c_2}$ e $\alpha_{12} \circ \alpha_{21} = id_{c_1}$. Portanto $c_1 \simeq c_2$. Para os objetos finais é análogo.

Exemplo 1.5.8. Algumas construções importantes:

(*i*) Sejam $\mathcal{C}$ uma categoria e $x, y \in Obj(\mathcal{C})$. Considere a categoria $x \leftarrow \mathcal{C} \to y$, cujos objetos são $\{x \xleftarrow{\alpha} c \xrightarrow{\beta} y \mid c \in Obj(\mathcal{C}),\ \alpha, \beta \in Mor(\mathcal{C})\}$ e os morfismos são setas $\varphi \in Hom_{\mathcal{C}}(c, c')$ que fazem o seguinte diagrama comutar:

$$\begin{tikzcd} x & c \arrow[l, "\alpha"'] \arrow[r, "\beta"] \arrow[d, "\varphi"] & y \\ & c' \arrow[ul, "\alpha'"] \arrow[ur, "\beta'"'] & \end{tikzcd}$$

O *produto de x e y*, denotado por $x \times y$, é o objeto final na categoria $x \leftarrow \mathcal{C} \to y$, quando ele existe. Essa definição coincide com as definições de produto nas categorias do exemplo 1.5.2.

(*ii*) Dada uma categoria $\mathcal{C}$ e dois objetos $x, y \in Obj(\mathcal{C})$, o *coproduto de x e y* é definido como o objeto inicial na categoria $x \to \mathcal{C} \leftarrow y$, quando ele existe. Denota-se o coproduto de x e y por $x \sqcup y$. Nas categorias **Sets** e **Top**, os coprodutos são simplesmente uniões disjuntas. Enquanto na categoria **Grp**, o coproduto é o produto livre de grupos.

(*iii*) Sejam $\mathcal{C}$ uma categoria e $c \in Obj(\mathcal{C})$ um objeto. Considere a categoria $\mathcal{C} \to c$, onde os objetos são $\{x \xrightarrow{\alpha} c \mid x \in Obj(\mathcal{C}), \alpha \in Mor(\mathcal{C})\}$ e os morfismos são morfismos $\varphi \in Hom_{\mathcal{C}}(x, y)$ que fazem o seguinte diagrama comutar:

$$\begin{tikzcd} x \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & c \\ y \arrow[ur, "\alpha'"'] & \end{tikzcd}$$

Para dois objetos $x, y \in Obj(\mathcal{C})$, define-se o *produto fibrado* (ou *pullback*) de x e y sobre c (denotado por $x \times_c y$) como o produto na categoria $\mathcal{C} \to c$, quando ele existe.

Nas categorias **Sets** e **Top**, o produto fibrado de $X \xrightarrow{\alpha} Z$ e $Y \xrightarrow{\beta} Z$ é $X \times_Z Y = \{(x, y) \in X \times Y \mid \alpha(x) = \beta(y)\}$. Na categoria **Grp**, o produto fibrado é o produto amalgamado de grupos.

(iv) Seja $\mathcal{C}$ uma categoria. O *pushout* é definido como o coproduto na categoria $c \to \mathcal{C}$, quando ele existe.

(v) Seja I um conjunto munido de uma ordem parcial $\leq$. O conjunto I é chamado de *conjunto dirigido* se, para quaisquer dois elementos $i, j \in I$, existe um elemento $k \in I$, tal que $i \leq k$ e $j \leq k$.

Sejam $\mathcal{C}$ uma categoria e $(I, \leq)$ um conjunto dirigido. Um *sistema dirigido* em $\mathcal{C}$ consiste de uma família de objetos, $\mathcal{X} = \{x_i \in Obj(\mathcal{C}) \mid i \in I\}$, e uma família de morfismos, $\mathcal{F} = \{f_{ij} : x_i \to x_j \mid i, j \in I,\ i \leq j\}$, satisfazendo as seguintes propriedades:

(a) $f_{ii} = id_{x_i}$, $\forall\ i \in I$;

(b) $f_{ik} = f_{jk} \circ f_{ij}$, $\forall\ i \leq j \leq k,\ i, j, k \in I$.

Seja $(\mathcal{X}, \mathcal{F})$ um sistema dirigido. Construa a categoria $\mathcal{C}'$ da seguinte forma. Considere a coleção de pares $(c, \{\varphi_i\})$, onde $c \in Obj(\mathcal{C})$ e $\{\varphi_i\}$ é uma família de morfismos $\{\varphi_i \in Hom_{\mathcal{C}}(x_i, c) \mid i \in I\}$, tais que os diagramas

$$\begin{tikzcd} x_i \arrow[rr, "f_{ij}"] \arrow[dr, "\varphi_i"'] & & x_j \arrow[dl, "\varphi_j"] \\ & c & \end{tikzcd}$$

comutam. Essa coleção será $Obj(\mathcal{C}')$. Considere também a coleção de morfismos $\xi \in Hom_{\mathcal{C}}(a, b)$ entre objetos da categoria $\mathcal{C}$ que comutam o diagrama

$$\begin{tikzcd} x_i \arrow[rr, "f_{ij}"] \arrow[dr, "\varphi_i"] \arrow[ddr, "\psi_i"'] & & x_j \arrow[dl, "\varphi_j"'] \arrow[ddl, "\psi_j"] \\ & a \arrow[d, "\xi"] & \\ & b & \end{tikzcd}$$

. Essa coleção será $Mor(\mathcal{C}')$. O objeto inicial da categoria $\mathcal{C}'$, quando ele existe, é chamado de *limite direto* do sistema dirigido $(\mathcal{X}, \mathcal{F})$.

(vi) Sejam $\mathcal{C}$ uma categoria e $(I, \leq)$ um conjunto dirigido. Um *sistema invertido* em $\mathcal{C}$ consiste de uma família de objetos, $\mathcal{X} = \{x_i \in Obj(\mathcal{C}) \mid i \in I\}$, e uma família de morfismos, $\mathcal{F} = \{f_{ji} : x_j \to x_i \mid i, j \in I,\ i \leq j\}$, satisfazendo as seguintes propriedades:

(a) $f_{ii} = id_{x_i}$, $\forall\ i \in I$;

(b) $f_{ki} = f_{ji} \circ f_{kj}$, $\forall\ i \leq j \leq k,\ i, j, k \in I$.

Seja $(\mathcal{X}, \mathcal{F})$ um sistema invertido. Construa a categoria $\mathcal{C}'$ da seguinte forma. Considere a coleção de pares $(c, \{\varphi_i\})$, onde $c \in Obj(\mathcal{C})$ e $\{\varphi_i\}$ é uma família de morfismos $\{\varphi_i \in Mor_{\mathcal{C}}(c, x_i) \mid i \in I\}$, tais que os diagramas

$$\begin{tikzcd} x_j \arrow[rr, "f_{ji}"] & & x_i \\ & c \arrow[ul, "\varphi_j"] \arrow[ur, "\varphi_i"'] & \end{tikzcd}$$

comutam. Essa coleção será $Obj(\mathcal{C}')$. Considere também a coleção de morfismos $\xi \in Mor_{\mathcal{C}}(b, a)$ entre objetos da categoria $\mathcal{C}$ que comutam o diagrama

$$\begin{tikzcd} x_j \arrow[rr, "f_{ji}"] & & x_i \\ & a \arrow[ul, "\varphi_j"'] \arrow[ur, "\varphi_i"] & \\ & b \arrow[u, "\xi"] \arrow[uul, "\psi_j"] \arrow[uur, "\psi_i"'] & \end{tikzcd}$$

. Essa coleção será $Mor(\mathcal{C}')$. O objeto inicial da categoria $\mathcal{C}'$, quando ele existe, é chamado de *limite inverso* do sistema dirigido $(\mathcal{X}, \mathcal{F})$.

Lema 1.5.9 (de Yoneda)**.** Sejam $\mathcal{C}$ uma categoria, $c \in Obj(\mathcal{C})$ um objeto e $F : \mathcal{C} \to \textbf{Sets}$ um funtor. A função $\eta : Hom(Hom_{\mathcal{C}}(c, \cdot), F) \to F(c)$ definida por $\eta(\alpha) = \alpha_c(id_c)$, para toda transformação natural $\alpha \in Hom(Hom(c, \cdot), F)$, é uma bijeção.

Capítulo 2

Álgebras de Lie semissimples

Neste capítulo serão abordadas álgebras de Lie semissimples e de dimensão finita sobre um corpo algebricamente fechado e de característica zero. Por isso, a partir de agora, denotaremos por $\mathbb{K}$ um corpo algebricamente fechado e de característica zero e toda $\mathbb{K}$-álgebra de Lie será considerada semissimples e de dimensão finita. A referência principal é [Hum1].

2.1 Álgebras torais

Definição 2.1.1. Sejam $\mathfrak{g}$ uma álgebra de Lie e $(\ ,\ )$ uma forma bilinear em $\mathfrak{g}$. A forma bilinear $(\ ,\ )$ é dita *invariante* quando $(\mathsf{x}, [\mathsf{y}, \mathsf{z}]) = ([\mathsf{x}, \mathsf{y}], \mathsf{z})$ para quaisquer $\mathsf{x}, \mathsf{y}, \mathsf{z} \in \mathfrak{g}$. O *radical* de $(\ ,\ )$ é o conjunto $\{\mathsf{g} \in \mathfrak{g} \mid (\mathsf{g}, \mathsf{x}) = 0,\ \forall\ \mathsf{x} \in \mathfrak{g}\}$. Uma forma bilinear simétrica é dita *não degenerada* quando o seu radical é nulo.

A forma bilinear definida por $(\mathsf{x}, \mathsf{y}) = Tr(ad(\mathsf{x}) \circ ad(\mathsf{y})),\ \forall\ \mathsf{x}, \mathsf{y} \in \mathfrak{g}$, é chamada de *forma de Cartan-Killing* em $\mathfrak{g}$. Uma álgebra de Lie é chamada de *semissimples* quando a forma de Cartan-Killing é não degenerada. Uma álgebra de Lie é chamada de *simples*, quando $\dim \mathfrak{g} > 1$ e $\mathfrak{g}$ não possui ideais próprios e não triviais.

Proposição 2.1.2.

(i) A forma de Cartan-Killing é simétrica e invariante.

(ii) Uma álgebra de Lie é semissimples se, e somente se, não existem ideais abelianos (como álgebras de Lie) não triviais.

(iii) Se $\mathfrak{g}$ é uma álgebra de Lie semissimples, então existem ideais simples (como álgebras de Lie), $I_1, \ldots, I_l \subseteq \mathfrak{g}$, tais que $\mathfrak{g} = I_1 \oplus \ldots \oplus I_l$. Todo ideal simples de $\mathfrak{g}$ coincide com algum I_j, $j \in \{1, \ldots, l\}$. A forma de Cartan-Killing em I_j é a restrição da forma em $\mathfrak{g} \times \mathfrak{g}$ para $I_j \times I_j$, $\forall\ j \in \{1, \ldots, l\}$.

(iv) Se uma álgebra de Lie é simples, então ela é semissimples.

Definição 2.1.3. Seja V um $\mathbb{K}$-espaço vetorial de dimensão finita. Uma transformação linear $T : V \to V$ é chamada de *semissimples* quando T for diagonalizável. A transformação linear T é chamada de *nilpotente* quando existir $n \in \mathbb{N}$, tal que T^n é a transformação nula.

Proposição 2.1.4. Sejam V um $\mathbb{K}$-espaço vetorial de dimensão finita e $\mathsf{x} : V \to V$ uma transformação linear. Então:

(i) Existem duas transformações lineares, $\mathsf{x}_s, \mathsf{x}_n : V \to V$, satisfazendo $\mathsf{x} = \mathsf{x}_s + \mathsf{x}_n$, onde x_s é semissimples, x_n é nilpotente e x_s comuta com x_n.

(ii) Tais x_n e x_s são únicos.

(iii) Existem dois polinômios $p(t), q(t) \in \mathbb{K}[t]$, tais que $p(\mathsf{x}) = \mathsf{x}_s$ e $q(\mathsf{x}) = \mathsf{x}_n$.

(iv) Se $U \subseteq W \subseteq V$ forem dois subespaços de V e $\mathsf{x}(W) \subseteq U$, então $\mathsf{x}_s(W), \mathsf{x}_n(W) \subseteq U$.

A proposição anterior é conhecida como Teorema de Jordan. A decomposição dos endomorfismos de V (descrita nesta proposição) em uma soma de endomorfismos semissimples e nilpotente é chamada de *decomposição de Jordan-Chevalley*.

Considere uma álgebra de Lie $\mathfrak{g}$. Observe que a representação adjunta define, para cada $\mathsf{x} \in \mathfrak{g}$, um endomorfismo de $\mathfrak{g}$, dado por $ad(\mathsf{x})$. Portanto é possível pensar na decomposição de Jordan-Chevalley de $ad(\mathsf{x})$.

Proposição 2.1.5. Sejam $\mathfrak{g}$ uma álgebra de Lie e $\mathsf{x} \in \mathfrak{g}$. Se $ad(\mathsf{x}) = ad(\mathsf{x})_s + ad(\mathsf{x})_n$ é a decomposição de Jordan-Chevalley de $ad(\mathsf{x})$, então $ad(\mathsf{x})_s, ad(\mathsf{x})_n \in im(ad)$. Como a representação adjunta é fiel, então existem únicos $\mathsf{s}, \mathsf{n} \in \mathfrak{g}$, tais que $ad(\mathsf{x})_n = ad(\mathsf{n})$ e $ad(\mathsf{x})_s = ad(\mathsf{s})$.

Definição 2.1.6. Sejam $\mathfrak{g}$ uma álgebra de Lie, x um elemento de $\mathfrak{g}$ e $ad(\mathsf{x}) = ad(\mathsf{s}) + ad(\mathsf{n})$ a decomposição de Jordan-Chevalley de $ad(\mathsf{x})$. Defina a *decomposição de Jordan-Chevalley* de $\mathsf{x} \in \mathfrak{g}$ como $\mathsf{x} = \mathsf{s} + \mathsf{n}$, onde s é chamado de *parte semissimples* e n é chamado de *parte nilpotente* de x.

Da definição acima fica claro que se a decomposição de Jordan-Chevalley de $\mathsf{x} \in \mathfrak{g}$ é $\mathsf{x} = \mathsf{x}_s + \mathsf{x}_n$, então a decomposição de Jordan-Chevalley de $ad(\mathsf{x})$ é $ad(\mathsf{x}) = ad(\mathsf{x}_s) + ad(\mathsf{x}_n)$. A proposição a seguir generaliza esse fato para uma representação qualquer de uma álgebra de Lie.

Proposição 2.1.7. Sejam $\mathfrak{g}$ uma álgebra de Lie, x um elemento de $\mathfrak{g}$ e $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ uma representação de dimensão finita de $\mathfrak{g}$. Se a decomposição de Jordan-Chevalley de x é $\mathsf{x} = \mathsf{x}_s + \mathsf{x}_n$, então a decomposição de Jordan-Chevalley de $\rho(\mathsf{x}) \in \mathfrak{gl}(V)$ é $\rho(\mathsf{x}) = \rho(\mathsf{x}_s) + \rho(\mathsf{x}_n)$.

Definição 2.1.8. Seja $\mathfrak{g}$ uma álgebra de Lie. Define-se uma *subálgebra toral maximal* como uma subálgebra maximal, no sentido da inclusão, dentre as subálgebras de $\mathfrak{g}$ que consistem somente de elementos semissimples.

Pela proposição 16.4 [Hum1], não há perda de generalidade em escolher e fixar uma subálgebra toral maximal de uma álgebra de Lie.

Proposição 2.1.9. Toda subálgebra toral maximal de uma álgebra de Lie é abeliana.

2.2 Sistemas de raízes

Considere $\mathfrak{g}$ uma álgebra de Lie com subálgebra toral maximal $\mathfrak{h}$ e uma representação de $\mathfrak{g}$ de dimensão finita $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$. Usando a proposição acima, é possível encontrar uma base para $\mathfrak{g}$ na qual todos os elementos de $\mathfrak{h}$ são diagonalizados simultaneamente. Usando, agora, a proposição 2.1.9, é possível encontrar uma base de V com respeito a qual $\rho(\mathfrak{h})$ age diagonalmente em V. Portanto é possível decompor $V = \bigoplus_\alpha V_\alpha$, onde $\alpha \in \mathfrak{h}^*$ e $V_\alpha = \{v \in V \mid \rho(\mathsf{h})(v) = \alpha(\mathsf{h})v, \ \forall\ \mathsf{h} \in \mathfrak{h}\}$. Em particular:

Proposição 2.2.1. Sejam $\mathfrak{g}$ uma álgebra de Lie e $\mathfrak{h}$ uma subálgebra toral maximal de $\mathfrak{g}$. Existem $\mathcal{R} \subseteq \mathfrak{h}^* \backslash \{0\}$ e subespaços vetoriais não triviais $\mathfrak{g}_\alpha \subseteq \mathfrak{g}$, $\alpha \in \mathcal{R}$, tais que $\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \mathcal{R}} \mathfrak{g}_\alpha$.

Considerando a representação adjunta, $ad : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$, os subespaços acima são os auto-espaços $\mathfrak{g}_\alpha = \{\mathsf{x} \in \mathfrak{g} \mid [\mathsf{h}, \mathsf{x}] = \alpha(\mathsf{h})\mathsf{x},\ \forall\ \mathsf{h} \in \mathfrak{h}\}$. Os elementos de $\mathcal{R}$ são chamados de *raízes* de $\mathfrak{g}$ e a decomposição $\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \mathcal{R}} \mathfrak{g}_\alpha$ é chamada de *decomposição de Cartan* de $\mathfrak{g}$.

Definição 2.2.2. Seja $\mathfrak{g}$ uma álgebra de Lie com subálgebra toral maximal $\mathfrak{h}$ e conjunto de raízes $\mathcal{R}$. Defina o *grupo de Weyl de* $\mathcal{R}$ como o grupo $\mathcal{W}$ gerado por $\{\sigma_\alpha \mid \alpha \in \mathcal{R}\}$, onde $\sigma_\alpha(x)$ é definido por $\sigma_\alpha(x) = x - 2\frac{(x,\alpha)}{(\alpha,\alpha)}$, $\forall\ x \in \mathfrak{h}^*$.

Proposição 2.2.3. Sejam $\mathfrak{g}$ uma álgebra de Lie, $\mathfrak{h}$ uma subálgebra toral maximal de $\mathfrak{g}$ e $\mathcal{R}$ o conjunto de raízes de $\mathfrak{g}$:

(*i*) Se $\alpha, \beta, (\alpha+\beta) \in \mathcal{R}$, então $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] = \mathfrak{g}_{\alpha+\beta}$. Se $\alpha, \beta \in \mathcal{R}$ e $\alpha+\beta \notin \mathcal{R}$, então $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] = 0$.

(*ii*) Se $\alpha, \beta \in \mathcal{R}$ e $\alpha+\beta \neq 0$, então $\mathfrak{g}_\alpha$ é ortogonal à $\mathfrak{g}_\beta$ em relação a forma de Cartan-Killing de $\mathfrak{g}$.

(*iii*) A forma de Cartan-Killing de $\mathfrak{g}$ restrita à $\mathfrak{h}$ é não degenerada. Portanto, pode-se identificar $\mathfrak{h}$ e $\mathfrak{h}^*$ da seguinte forma: a cada $\alpha \in \mathfrak{h}^*$, associe o elemento $\mathsf{t}_\alpha \in \mathfrak{h}$ que satisfaz $(\mathsf{t}_\alpha, \cdot) = \alpha$.

(*iv*) $\mathcal{R}$ gera $\mathfrak{h}^*$.

(*v*) Para todo $w \in \mathcal{W}$ e $\alpha \in \mathcal{R}$, $w(\alpha) \in \mathcal{R}$.

(*vi*) Se $\alpha \in \mathcal{R}$ e $\lambda \in \mathbb{K}$, então $\lambda\alpha \in \mathcal{R}$ se, e somente se, $\lambda = \pm 1$.

(*vii*) $\dim(\mathfrak{g}_\alpha) = 1$, $\forall\ \alpha \in \mathcal{R}$.

(*viii*) Para cada $\alpha \in \mathcal{R}$, considere $\mathsf{h}_\alpha := \frac{2\mathsf{t}_\alpha}{(\mathsf{t}_\alpha, \mathsf{t}_\alpha)}$. Para todo $\mathsf{x}_\alpha \in \mathfrak{g}_\alpha$, existe um único $\mathsf{y}_\alpha \in \mathfrak{g}_{-\alpha}$, tal que $[\mathsf{x}_\alpha, \mathsf{y}_\alpha] = \mathsf{h}_\alpha$.

(*ix*) Para todo $\alpha, \beta \in \mathcal{R}$, $\alpha(\mathsf{h}_\beta) = \frac{2(\alpha,\beta)}{(\beta,\beta)} \in \mathbb{Z}$. Em particular, $[\mathsf{h}_\beta, \mathsf{x}_\alpha] = \alpha(\mathsf{h}_\beta)\mathsf{x}_\alpha \in \mathbb{Z}x_\alpha$.

Essas propriedades permitem que se axiomatize os possíveis conjuntos de raízes, ou seja, conjuntos de funcionais lineares cujos auto-espaços formam uma decomposição de Cartan de álgebras de Lie.

Definição 2.2.4. Um subconjunto $\mathcal{R}$ de um espaço euclidiano $(E, (\ ,\ ))$ é chamado de *sistema de raízes* em E se satisfaz as seguintes condições:

(*i*) $\mathcal{R}$ é um conjunto finito de geradores de E que não contém zero.

(*ii*) Se $\alpha \in \mathcal{R}$, então os únicos múltiplos escalares de α em $\mathcal{R}$ são $\pm\alpha$.

(*iii*) Para todo $\alpha \in \mathcal{R}$, as reflexões do espaço E dadas por $\sigma_\alpha(x) = x - 2\frac{(x,\alpha)}{(\alpha,\alpha)}\alpha$ deixam $\mathcal{R}$ invariante.

(*iv*) Para quaisquer $\beta, \alpha \in \mathcal{R}$, $\langle \beta, \alpha \rangle := 2\frac{(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$.

O grupo formado pelas reflexões $\{\sigma_\alpha \mid \alpha \in \mathcal{R}\}$ também é chamado de *grupo de Weyl de* $\mathcal{R}$.

Sejam $(E_1, (\ ,\ )_1)$ e $(E_2, (\ ,\ )_2)$ dois espaços euclidianos e $\mathcal{R}_1$ e $\mathcal{R}_2$ dois sistemas de raízes em E_1 e E_2 respectivamente. Um *isomorfismo* entre os dois sistemas de raízes é um isomorfismo linear $\varphi : E_1 \to E_2$ tal que $\varphi(\mathcal{R}_1) = \mathcal{R}_2$ e $(\alpha, \beta)_1 = (\varphi(\alpha), \varphi(\beta))_2$, $\forall\ \alpha, \beta \in \mathcal{R}_1$.

Observe que pela proposição 2.2.3 o conjunto de raízes definido após a proposição 2.2.1 é um sistema de raízes no sentido da definição 2.2.4 onde E é o espaço $\mathbb{R}$-gerado por $\mathcal{R}$.

Mais adiante será visto que todo sistema de raízes no sentido da definição 2.2.4 pode ser realizado como conjunto de raízes de uma álgebra de Lie como definido após a proposição 2.2.1.

Definição 2.2.5. Seja $\mathcal{R}$ um sistema de raízes em um espaço Euclidiano E. Um subconjunto $\mathcal{B} \subseteq \mathcal{R}$ é chamado de *base* de $\mathcal{R}$, quando:

(*i*) $\mathcal{B}$ é uma base para E.

(*ii*) Toda raiz $\alpha \in \mathcal{R}$ pode ser escrita como $\alpha = \sum_i z_i \beta_i$, onde $\beta_i \in \mathcal{B}$ e z_i são inteiros todos não-positivos ou todos não-negativos.

As raízes pertencentes a base são chamadas de *raízes simples* (em relação a $\mathcal{B}$).

Fixando uma base $\mathcal{B}$, as raízes de $\mathcal{R}$ que são escritas como combinações lineares dessa base com coeficientes inteiros não-negativos são chamadas de *raízes positivas*, enquanto as raízes de $\mathcal{R}$ que são escritas como combinações lineares dessa base com coeficientes inteiros não-positivos são chamadas de raízes negativas. Denota-se o conjunto de raízes positivas por $\mathcal{R}^+$ e de raízes negativas por $\mathcal{R}^-$. Do axioma (*ii*) da definição de sistema de raízes, conclui-se que $\mathcal{R}^+ = -\mathcal{R}^-$.

O $\mathbb{Z}$-submódulo de E gerado por $\mathcal{R}$ (equivalentemente, por $\mathcal{B}$), é chamado de *reticulado de raízes* e denotado por $\mathcal{Q}$. O conjunto $\mathbb{N}$-gerado por $\mathcal{R}$ (equivalentemente, por $\mathcal{B}$) em E é chamado de *cone de raízes positivas* e denotado por $\mathcal{Q}^+$. Define-se uma ordem parcial em E da seguinte forma: $\lambda \leq \mu$, quando $\mu - \lambda \in \mathcal{Q}^+$.

Teorema 2.2.6. Seja $\mathcal{R}$ um sistema de raízes em um espaço Euclidiano E. Então existe uma base para $\mathcal{R}$.

A partir de agora, considere o caso em que o espaço euclidiano E é $\mathbb{R}$-gerado por $\mathcal{R}$.

Lema 2.2.7. Seja $\mathfrak{g}$ uma álgebra de Lie com sistema de raízes $\mathcal{R}$ e base $\mathcal{B}$. Se $\alpha_1, \alpha_2 \in \mathcal{B}$ e $\langle \alpha_1, \alpha_2 \rangle \langle \alpha_2, \alpha_1 \rangle > 1$, então ou $(\alpha_1, \alpha_1) > (\alpha_2, \alpha_2)$, ou $(\alpha_2, \alpha_2) > (\alpha_1, \alpha_1)$.

Definição 2.2.8. Seja $\mathfrak{g}$ uma álgebra de Lie com sistema de raízes $\mathcal{R}$ e base $\mathcal{B}$ dada por $\{\alpha_1, \ldots, \alpha_l\}$. A matriz de Cartan de $\mathfrak{g}$ é definida por $A = (a_{ij})$ com $a_{ij} = \langle \alpha_i, \alpha_j \rangle$.

O *diagrama de Dynkin* associado a matriz de Cartan A é um grafo contendo l vértices (indexados pelas raízes simples), tais que os vértices associados às raízes α_i e α_j são ligados entre si por $a_{ij}a_{ji}$ arestas. Quando existe mais de uma aresta ligando dois vértices, adiciona-se uma seta apontando para a menor raiz, com relação a norma induzida da forma de Cartan-Killing (ou, o que é equivalente, um sinal de desigualdade discriminando a relação de ordem entre as raízes relacionadas aos vértices).

Proposição 2.2.9. A matriz de Cartan tem a seguinte forma:

(*i*) $a_{ii} = 2$ para todo $i = 1, \dots, l$.

(*ii*) $a_{ij} \in \{0, -1, -2, -3\}$, $\forall\ 1 \leq i \neq j \leq l$.

(*iii*) se $a_{ij} = 0$, então $a_{ji} = 0$, $\forall\ 1 \leq i, j \leq l$.

(*iv*) se $a_{ij} = -2, -3$, então $a_{ji} = -1$, $\forall\ 1 \leq i, j \leq l$.

A matriz de Cartan determina o diagrama de Dynkin unicamente.

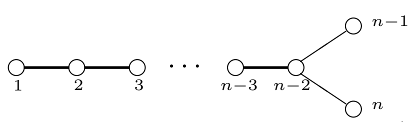
Exemplo 2.2.10. Diagramas de Dynkin e matrizes de Cartan das álgebras clássicas:

$\mathfrak{sl}_{n+1}$: 

$$\begin{pmatrix} 2 & -1 & 0 & \dots & \dots & \dots & 0 \\ -1 & 2 & -1 & 0 & \dots & \dots & 0 \\ 0 & -1 & 2 & -1 & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & \ddots & & \vdots \\ 0 & \dots & 0 & -1 & 2 & -1 & 0 \\ 0 & \dots & \dots & 0 & -1 & 2 & -1 \\ 0 & \dots & \dots & \dots & 0 & -1 & 2 \end{pmatrix}$$

$\mathfrak{so}_{2n+1}$: 

$$\begin{pmatrix} 2 & -1 & 0 & \dots & \dots & \dots & 0 \\ -1 & 2 & -1 & 0 & \dots & \dots & 0 \\ 0 & -1 & 2 & -1 & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & \ddots & & \vdots \\ 0 & \dots & 0 & -1 & 2 & -1 & 0 \\ 0 & \dots & \dots & 0 & -1 & 2 & -2 \\ 0 & \dots & \dots & \dots & 0 & -1 & 2 \end{pmatrix}$$

$\mathfrak{so}_{2n}$: 

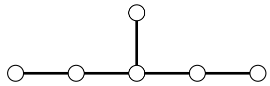
$$\begin{pmatrix} 2 & -1 & 0 & \dots & \dots & \dots & 0 \\ -1 & 2 & -1 & 0 & \dots & \dots & 0 \\ 0 & -1 & 2 & -1 & \dots & \dots & 0 \\ & & \ddots & \ddots & \ddots & & \\ 0 & \dots & -1 & 2 & -1 & 0 & 0 \\ 0 & \dots & \dots & -1 & 2 & -1 & -1 \\ 0 & \dots & \dots & \dots & -1 & 2 & 0 \\ 0 & \dots & \dots & \dots & -1 & 0 & 2 \end{pmatrix}$$

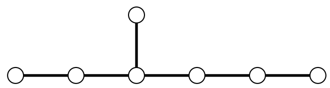
$\mathfrak{sp}_{2n}$: 

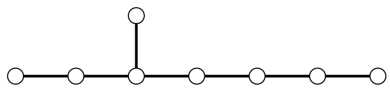
$$\begin{pmatrix} 2 & -1 & 0 & \dots & \dots & \dots & 0 \\ -1 & 2 & -1 & 0 & \dots & \dots & 0 \\ 0 & -1 & 2 & -1 & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & \ddots & & \vdots \\ 0 & \dots & 0 & -1 & 2 & -1 & 0 \\ 0 & \dots & \dots & 0 & -1 & 2 & -1 \\ 0 & \dots & \dots & \dots & 0 & -2 & 2 \end{pmatrix}$$

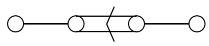
Proposição 2.2.11. A matriz de Cartan determina o sistema de raízes a menos de isomorfismo.

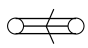
Veremos a seguir que as álgebras de Lie semissimples são unicamente determinadas pelo seu sistema de raízes a menos de isomorfismo. Assim sendo, classificar todas as álgebras de Lie simples é equivalente a classificar os possíveis diagramas de Dynkin conexos. Considere o espaço euclidiano $(E, (\ ,\ ))$ $\mathbb{R}$-gerado por $\mathcal{R}$ e munido da forma de Cartan-Killing. Para classificar os possíveis diagramas de Dynkin, usa-se geometria Euclidiana básica sobre conjuntos de vetores da base de $\mathcal{R}$ e exige-se que eles satisfaçam as condições sobre os ângulos entre eles decorrentes de 2.2.9. Como conclusão, os possíveis diagramas de Dynkin são os diagramas das álgebras clássicas, descritos no exemplo 2.2.10 e os seguintes diagramas excepcionais:

E_6 : 

E_7 : 

E_8 : 

F_4 : 

G_2 : 

Teorema 2.2.12 (de Serre)**.** Considere uma matriz de Cartan $A = (a_{ij})$, $1 \leq i, j \leq l$. Seja $\mathfrak{g}$ a álgebra de Lie gerada por $3l$ elementos, $\{\mathsf{x}_i, \mathsf{y}_i, \mathsf{h}_i \mid i = 1, \ldots, l\}$, satisfazendo as seguintes relações:

(i) $[\mathsf{h}_i, \mathsf{h}_j] = 0$, $\forall\ 1 \leq i, j \leq l$;

(ii) $[\mathsf{h}_i, \mathsf{x}_j] = a_{ij}\mathsf{x}_j$, $\quad [\mathsf{h}_i, \mathsf{y}_j] = -a_{ij}\mathsf{y}_j$, $\forall\ 1 \leq i, j \leq l$;

(iii) $[\mathsf{x}_i, \mathsf{y}_j] = \delta_{ij}\mathsf{h}_i$, $\forall\ 1 \leq i, j \leq l$;

(iv) $(ad(\mathsf{x}_i))^{1-a_{ij}}(\mathsf{x}_j) = 0$, $\quad (ad(\mathsf{y}_i))^{1-a_{ij}}(\mathsf{y}_j) = 0$, $\forall\ 1 \leq i \neq j \leq l$.

Então $\mathfrak{g}$ é uma álgebra de Lie semissimples e de dimensão finita, com subálgebra toral maximal gerada por $\{\mathsf{h}_i \mid i = 1, \ldots, l\}$.

As álgebras de Lie simples dadas pelo teorema de Serre a partir dos diagramas E_6, E_7, E_8, F_4 e G_2 são chamadas de *álgebras excepcionais* e são denotadas por $\mathfrak{e}_6$, $\mathfrak{e}_7$, $\mathfrak{e}_8$, $\mathfrak{f}_4$ e $\mathfrak{g}_2$ respectivamente. Com isso, obtemos a seguinte classificação.

Corolário 2.2.13. Se $\mathfrak{g}$ é uma álgebra de Lie simples e de dimensão finita sobre um corpo algebricamente fechado de característica zero, então $\mathfrak{g}$ é isomorfa a: $\mathfrak{sl}_n$, $\mathfrak{sp}_{2n}$, $\mathfrak{so}_n$, $\mathfrak{e}_6$, $\mathfrak{e}_7$, $\mathfrak{e}_8$, $\mathfrak{f}_4$ ou $\mathfrak{g}_2$.

2.3 Forma de Kostant

Definição 2.3.1. Sejam $\mathfrak{g}$ uma álgebra de Lie com uma subálgebra toral maximal $\mathfrak{h}$ e um sistema de raízes $\mathcal{R}$ com base $\mathcal{B} = \{\alpha_1, \ldots, \alpha_l\}$. Define-se um *peso de* $\mathfrak{g}$ como um elemento $\lambda \in \mathfrak{h}^*$, tal que, para todo $\alpha \in \mathcal{R}$, $\langle \lambda, \alpha \rangle \in \mathbb{Z}$ ou, equivalentemente, $\lambda(\mathsf{h}_{\alpha_i}) \in \mathbb{Z}, \forall\ i = 1, \ldots, l$.

Defina por $\lambda_i \in \mathfrak{h}^*$, os pesos que satisfazem $\lambda_i(\mathsf{h}_{\alpha_j}) = \delta_{ij}$ para cada $i, j \in \{1 \ldots, l\}$. O conjunto $\{\lambda_1, \ldots, \lambda_l\}$ é chamado de conjunto de *pesos fundamentais*. O conjunto $\mathcal{P}$ dos pesos de $\mathfrak{g}$ é um $\mathbb{Z}$-submódulo de $\mathfrak{h}^*$ gerado livremente pelos pesos fundamentais e chamado de *reticulado de pesos*.

Um peso é chamado de *dominante*, quando $\lambda = \sum_i k_i\lambda_i \in \mathcal{P}$ e $k_i \geq 0$ para todo $i \in \{1, \ldots, l\}$ ou, equivalentemente, $\langle \lambda, \beta_i \rangle \in \mathbb{N}$ para todo $\beta_i \in \mathcal{B}$. O conjunto de pesos dominantes é denotado por $\mathcal{P}^+$.

Observe que pelo quarto axioma da definição 2.2.4, toda raiz é um peso.

Definição 2.3.2. Sejam $\mathfrak{g}$ uma álgebra de Lie com subálgebra toral maximal $\mathfrak{h}$ e $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ uma representação de $\mathfrak{g}$. Chamam-se *subespaços de peso*, os auto-espaços $V_\lambda = \{v \in V \mid \rho(\mathsf{h}).v = \lambda(\mathsf{h})v,\ \forall\ \mathsf{h} \in \mathfrak{h}\}$. Definem-se os *pesos da representação* V como os funcionais $\lambda \in \mathfrak{h}^*$, tais que $V_\lambda \neq \{0\}$.

O conjunto de pesos de uma representação (V, ρ) será denotado por $\Pi(V, \rho)$. O $\mathbb{Z}$-submódulo de $\mathfrak{h}^*$ gerado por $\Pi(V, \rho)$ será denotado por $\Lambda(V, \rho)$ e chamado de *reticulado de pesos*.

Se (V, ρ) for uma representação fiel de $\mathfrak{g}$, então $\mathcal{Q} \subseteq \Lambda(V, \rho) \subseteq \mathcal{P}$.

Exemplo 2.3.3.

(i) Considere a representação $\rho_0 : \mathfrak{sl}_2 \to \mathfrak{gl}_2(1.4.11\ (ii))$, onde cada matriz age como multiplicação de matriz por vetor. Considere a base para $\mathfrak{sl}_2$ dada por

$$\mathsf{y} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \mathsf{h} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathsf{x} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

A subálgebra toral maximal de $\mathfrak{sl}_2$ é a subálgebra gerada por h. Como h é diagonal, os pesos da representação são $\Pi(V, \rho_0) = \{-1, 1\}$. O reticulado de pesos, ou seja, o $\mathbb{Z}$-módulo gerado pelos pesos é $\Lambda(V, \rho_0) \simeq \mathbb{Z}$. Portanto o reticulado de pesos de (V, ρ_0) coincide com o reticulado de pesos de $\mathfrak{sl}_2$.

(ii) Cosidere a representação adjunta de $\mathfrak{sl}_2$, como no exemplo 1.4.11 (i). Considere a base para $\mathfrak{sl}_2$ dada por $\{\mathsf{y}, \mathsf{h}, \mathsf{x}\}$ como no item anterior. Como h gera a subálgebra toral maximal, basta calcular os auto-valores da imagem de h pela adjunta, a saber

$$ad(\mathsf{h}) = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Portanto os pesos da representação adjunta de $\mathfrak{sl}_2$ são $\Pi(\mathfrak{sl}_2, ad) = \{-2, 0, 2\}$. O reticulado de pesos da representação adjunta de $\mathfrak{sl}_2$, ou seja, o $\mathbb{Z}$-módulo gerado por $\{-2, 0, 2\}$ é $\Lambda(\mathfrak{sl}_2, ad) \simeq 2\mathbb{Z}$. Portanto o reticulado de pesos da representação adjunta de $\mathfrak{sl}_2$ coincide com o reticulado de raízes de $\mathfrak{sl}_2$.

Definição 2.3.4. Sejam $\mathfrak{g}$ uma álgebra de Lie com sistema de raízes $\mathcal{R}$. Para cada $\alpha, \beta \in \mathcal{R}$, defina a *$\alpha$-cadeia através de β* como o subconjunto de raízes da forma: $\beta + n\alpha \in \mathcal{R}$, $n \in \mathbb{Z}$.

Proposição 2.3.5. Seja $\mathfrak{g}$ uma álgebra de Lie com sistema de raízes $\mathcal{R}$. Existem $\mathsf{x}_\alpha \in \mathfrak{g}_\alpha$, $\alpha \in \mathcal{R}$, satisfazendo:

(i) $[\mathsf{x}_\alpha, \mathsf{x}_{-\alpha}] = \mathsf{h}_\alpha$, $\forall\ \alpha \in \mathcal{R}$;

(ii) Se $\alpha, \beta, (\alpha + \beta) \in \mathcal{R}$ e $[\mathsf{x}_\alpha, \mathsf{x}_\beta] = c_{\alpha,\beta}\mathsf{x}_{\alpha+\beta}$, então $c_{\alpha,\beta} \in \mathbb{Z}$ e $c_{\alpha,\beta} = -c_{-\alpha,-\beta}$.

Além disso, para qualquer escolha de vetores $\mathsf{x}_\alpha \in \mathfrak{g}_\alpha$, os escalares $c_{\alpha,\beta}$ satisfazem:

(iii) $c^2_{\alpha,\beta} = z(1 - a)\frac{(\alpha+\beta,\alpha+\beta)}{(\beta,\beta)}$, onde $\alpha + a\beta, \ldots, \alpha + z\beta$ é a α-cadeia através de β.

Definição 2.3.6. Seja $\mathfrak{g}$ uma álgebra de Lie. Uma base de $\mathfrak{g}$, $\{\mathsf{x}_\alpha, \mathsf{y}_\alpha, \mathsf{h}_i \mid \alpha \in \mathcal{R}^+ \ e\ i \in I\}$, tal que I é o conjunto de vértices do diagrama de Dynkin de $\mathfrak{g}$, $\mathsf{y}_\alpha = \mathsf{x}_{-\alpha}$ e os elementos da base satisfazem as codições da proposição 2.3.5 é chamada de *base de Chevalley*.

Teorema 2.3.7 (de Chevalley)**.** Seja $\mathfrak{g}$ uma álgebra de Lie com base de Chevalley $\{\mathsf{x}_\alpha, \mathsf{y}_\alpha, \mathsf{h}_i \mid \alpha \in \mathcal{R}^+ \ e\ i \in I\}$, onde I é o conjunto de vértices do diagrama de Dynkin de $\mathfrak{g}$ e $\mathcal{R}$ seu sistema de raízes. Então:

(*i*) $[\mathsf{h}_i, \mathsf{h}_j] = 0, \ \forall\ i, j \in I$;

(*ii*) $[\mathsf{h}_i, \mathsf{x}_\alpha] = \alpha(\mathsf{h}_i)\mathsf{x}_\alpha$, $[\mathsf{h}_i, \mathsf{y}_\alpha] = -\alpha(\mathsf{h}_i)\mathsf{y}_\alpha$, $\forall\ \alpha \in \mathcal{R}^+,\ i \in I$;

(*iii*) $[\mathsf{x}_\alpha, \mathsf{y}_\alpha] = \mathsf{h}_\alpha$, onde h_α é uma combinação $\mathbb{Z}$-linear dos h_i, $\forall\ \alpha \in \mathcal{R}^+$;

(*iv*) Se $\alpha, \beta \in \mathcal{R}$, $\alpha \neq \pm\beta$ e $\alpha + a\beta, \dots, \alpha + z\beta$ é a α-cadeia através de β, então: $[\mathsf{x}_\alpha, \mathsf{x}_\beta] = 0$, se $z = 0$ e $[\mathsf{x}_\alpha, \mathsf{x}_\beta] = \pm(1 - a)\mathsf{x}_{\alpha+\beta}$, se $\alpha + \beta \in \mathcal{R}$.

O teorema a seguir foi provado por Kostant em [Kos]. Para esse teorema, considere $\mathfrak{g}$ uma álgebra de Lie com subálgebra toral maximal $\mathfrak{h}$, $\dim \mathfrak{h} = l$ e sistema de raízes $\mathcal{R}$. Além disso, fixe uma ordem para o conjunto $\mathcal{R}^+ = \{\alpha_1, \dots, \alpha_m\}$. Denote $A = (a_1, \dots, a_m) \in \mathbb{N}^m$, $B = (b_1, \dots, b_l) \in \mathbb{N}^l$ e $C = (c_1, \dots, c_m) \in \mathbb{N}^m$. Denote os seguintes elementos de $U(\mathfrak{g})$: $e_C = \frac{\mathsf{x}_{\alpha_1}^{c_1}}{c_1!} \dots \frac{\mathsf{x}_{\alpha_m}^{c_m}}{c_m!}$, $f_A = \frac{\mathsf{y}_{\alpha_1}^{a_1}}{a_1!} \dots \frac{\mathsf{y}_{\alpha_m}^{a_m}}{a_m!}$ e $h_B = \binom{\mathsf{h}_1}{b_1} \dots \binom{\mathsf{h}_l}{b_l}$, onde $\binom{\mathsf{h}_k}{b_k} = \frac{\mathsf{h}_k(\mathsf{h}_k-1)\dots(\mathsf{h}_k-b_k+1)}{k!}$. Denote o conjunto $\{f_A h_B e_C \mid A \in \mathbb{N}^m,\ B \in \mathbb{N}^l \ e\ C \in \mathbb{N}^m\}$ por $\mathtt{C}$.

Teorema 2.3.8 (de Kostant)**.** Seja $U(\mathfrak{g})_\mathbb{Z}$ o subanel de $U(\mathfrak{g})$ (com unidade) gerado por $\{\frac{\mathsf{x}_\alpha^j}{j!}, \frac{\mathsf{y}_\alpha^j}{j!} \mid \alpha \in \mathcal{R}^+,\ j \in \mathbb{N}\}$. Seja $\mathfrak{B}$ o $\mathbb{Z}$-submódulo de $U(\mathfrak{g})$ gerado por $\mathtt{C}$. Então $U(\mathfrak{g})_\mathbb{Z} = \mathfrak{B}$. Em particular, $U(\mathfrak{g})_\mathbb{Z}$ é um $\mathbb{Z}$-submódulo de $U(\mathfrak{g})$ livremente gerado por $\mathtt{C}$.

Definição 2.3.9. A $\mathbb{Z}$-subálgebra (com unidade) de $U(\mathfrak{g})$ gerada por $\mathtt{C}$ é chamada de *forma integral de Kostant*.

Definição 2.3.10. Seja V um $\mathbb{K}$-espaço vetorial de dimensão finita. Define-se um *reticulado* em V como um $\mathbb{Z}$-submódulo livremente gerado por uma $\mathbb{K}$-base de V.

Sejam $\mathfrak{g}$ uma álgebra de Lie e $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ uma representação de dimensão finita. Um reticulado $\mathcal{L}$ em V é chamado de *admissível* quando for invariante pela ação de $U(\mathfrak{g})_\mathbb{Z}$ (definida no Teorema de Kostant), ou equivalentemente, quando ρ induz uma representação de $U(\mathfrak{g})_\mathbb{Z}$ em $\mathcal{L}$.

Teorema 2.3.11. Sejam $\mathfrak{g}$ uma álgebra de Lie e $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ uma representação de $\mathfrak{g}$ de dimensão finita. Existe um reticulado admissível em V. Se $\mathcal{L}$ for um tal reticulado admissível de V, então $\mathcal{L} = \bigoplus_{\lambda \in \Pi(V,\rho)} \mathcal{L} \cap V_\lambda$, ou seja, todo reticulado admissível pode ser decomposto como soma direta das suas intersecções com os subespaços de peso de V.

Exemplo 2.3.12. Alguns reticulados admissíveis.

(*i*) Para qualquer álgebra de Lie $\mathfrak{g}$, uma base de Chevalley gera um reticulado admissível em $\mathfrak{g}$ para a representação adjunta.

(*ii*) Para a representação $\rho_0 : \mathfrak{sl}_2 \to \mathfrak{gl}_2$ (como descrita no exemplo 1.4.11 (*ii*)), o reticulado $\mathcal{L} = \mathbb{Z}(1,0) \oplus \mathbb{Z}(0,1)$ é admissível, pois $\mathsf{h} \in \mathfrak{sl}_2$ decompõe V em $V_{-1} \oplus V_1$, onde V_{-1} é gerado por $(0,1)$, enquanto V_1 é gerado por $(1,0)$ e $\rho_0(\mathsf{y})(e_1) = e_2$, enquanto $\rho_0(\mathsf{x})(e_2) = e_1$.

Proposição 2.3.13. Sejam $\mathfrak{g}$ uma álgebra de Lie, $\alpha \in \mathcal{R}$ uma raiz de $\mathfrak{g}$, $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ uma representação de $\mathfrak{g}$ de dimensão finita e $\mathcal{L}$ um reticulado admissível em V. Se $v \in (\mathcal{L} \cap V_\lambda)$ e $\mathsf{x} \in \mathfrak{g}_\alpha$, então $\rho(\mathsf{x})(v) \in (\mathcal{L} \cap V_{\lambda+\alpha})$.

Notação 2.3.14. Sejam $\mathfrak{g}$ uma álgebra de Lie com subálgebra toral maximal $\mathfrak{h}$ e $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ uma representação fiel de dimensão finita de $\mathfrak{g}$. Denote por $\mathcal{L}_\mathbb{Z}$ um reticulado admissível de V. Denote por $\mathfrak{g}_\rho$ a subálgebra de $\mathfrak{g}$ que estabiliza $\mathcal{L}_\mathbb{Z}$. Analogamente, denote por $\mathfrak{h}_\rho$ a subálgebra de $\mathfrak{h}$ que estabiliza $\mathcal{L}_\mathbb{Z}$, isto é, $\mathfrak{h}_\rho = \{\mathsf{h} \in \mathfrak{h} \mid \lambda(\mathsf{h}) \in \mathbb{Z},\ \forall\ \lambda \in \Pi(V,\rho)\}$.

A notação do estabilizador parece estranha por explicitar a representação e não explicitar o reticulado que é estabilizado. No entanto, segundo a seguinte proposição, provada em [Ste], isso não causa nenhuma ambiguidade:

Proposição 2.3.15. Sejam $\mathfrak{g}$ uma álgebra de Lie e $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ uma representação fiel de dimensão finita de $\mathfrak{g}$. Para qualquer reticulado admissível $\mathcal{L}_\mathbb{Z}$ de V, o seu estabilizador $\mathfrak{g}_\rho$ é um reticulado admissível para a representação adjunta e se decompõe da seguinte forma:

$$\mathfrak{g}_\rho = \left(\bigoplus_{\alpha \in \mathcal{R}^+} \mathbb{Z}\mathsf{y}_\alpha \right) \oplus \mathfrak{h}_\rho \oplus \left(\bigoplus_{\alpha \in \mathcal{R}^+} \mathbb{Z}\mathsf{x}_\alpha \right).$$

Essa proposição mostra, em particular, que $\mathfrak{g}_\rho$ é de fato independente do reticulado e depende somente da representação. Mais precisamente, o estabilizador depende somente do seu reticulado de pesos, para determinar $\mathfrak{h}_\rho$.

Exemplo 2.3.16. Estabilizadores dos reticulados admissíveis de $\mathfrak{sl}_2$ descritos no exemplo anterior.

(*i*) Para a representação adjunta de $\mathfrak{sl}_2$, $\mathfrak{g}_\rho = \mathbb{Z}.\mathsf{y} \oplus \mathbb{Z}.(\mathsf{h}/2) \oplus \mathbb{Z}.\mathsf{x}$ é o estabilizador.

(*ii*) Para a representação $\rho_0 : \mathfrak{sl}_2 \to \mathfrak{gl}_2$, $\mathfrak{g}_{\rho_0} = \mathbb{Z}.\mathsf{y} \oplus \mathbb{Z}.\mathsf{h} \oplus \mathbb{Z}.\mathsf{x}$ é o estabilizador.

Capítulo 3

Variedades Algébricas

3.1 Definições, exemplos e propriedades

Variedades algébricas podem ser vistas de várias formas. Esta seção tem por fim descrevê-las de algumas destas várias formas, desde o mais palpável, como conjuntos de pontos satisfazendo algumas propriedades algébricas, até o "abstract non-sense", como funtores representáveis na categoria de álgebras. As referências para as definições e para os resultados são [Hum2], [Har] e [Jan].

Durante toda esta seção, assuma que $\mathbb{K}$ é um corpo algebricamente fechado.

3.1.1 Variedades afins

Definição 3.1.1. Defina o *espaço afim n-dimensional* como o conjunto de n-uplas de elementos em $\mathbb{K}$ e denote-o por $\mathbb{A}^n$.

Definição 3.1.2. Seja $\mathbb{K}[x_1, \ldots, x_n]$ o anel de polinômios em n variáveis sobre $\mathbb{K}$. Para cada ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ defina a *variedade afim associada a I* como o conjunto

$$V(I) = \{x \in \mathbb{A}^n \mid f(x) = 0, \ \forall\ f \in I\}.$$

Reciprocamente, para todo subconjunto $X \subseteq \mathbb{A}^n$, defina o *ideal associado a X* como

$$I(X) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(x) = 0, \ \forall\ x \in X\}.$$

Proposição 3.1.3. Sejam X, Y subconjuntos do espaço afim $\mathbb{A}^n$ e I, J ideais de $\mathbb{K}[x_1, \ldots, x_n]$.

(i) Se $Y \subseteq X$, então $I(Y) \supseteq I(X)$.

(ii) Se $I \subseteq J$, então $V(I) \supseteq V(J)$.

(iii) $I(\mathbb{A}^n) = \{0\}$.

(iv) $V(\mathbb{K}[x_1, \ldots, x_n]) = \emptyset$.

(v) $X \subseteq V(I(X))$.

(vi) $J \subseteq I(V(J))$.

(*vii*) $I(X)$ é um ideal radical.

Dem: (*i*) Como $Y \subseteq X$, se um polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ anula todos os elementos de X, então f anula todos os elementos de Y também. Ou seja, se $f \in I(X)$, então $f \in I(Y)$. Portanto $I(X) \subseteq I(Y)$.

(*ii*) Como $I \subseteq J$, se um ponto $x \in \mathbb{A}^n$ é anulado por todos os polinômios de J, então x é anulado por todos os polinômios de I. Ou seja, se $x \in V(J)$, então $x \in V(I)$. Portanto $V(J) \subseteq V(I)$.

(*iii*) É claro que $0 \in I(\mathbb{A}^n)$. Por outro lado, como o corpo $\mathbb{K}$ é algebricamente fechado, $\mathbb{K}$ contém uma quantidade infinita de pontos. A fortiori $\mathbb{A}^n$ também contém uma quantidade infinita de pontos. Seja $f \in \mathbb{K}[x_1, \ldots, x_n]$ um polinômio que se anula em todo ponto de $\mathbb{A}^n$. Se $n = 1$, então f é um polinômio em uma variável com uma quantidade infinita de zeros. Consequentemente, $f = 0$. Vamos usar indução para n qualquer. Decomponha

$$f = \sum_{i=0}^{d} f_i(x_1, \ldots, x_{n-1}) x_n^i,$$

onde $f_i(x_1, \ldots, x_{n-1}) \in \mathbb{K}[x_1, \ldots, x_{n-1}]$ para todo $i = 1, \ldots, d$, onde d é o grau de f. Como $f(a) = 0$ para todo $a \in \mathbb{A}^n$, $f_i(b) = 0$ para todo $b \in \mathbb{A}^{n-1}$. Usando a hipótese de indução, $f_i = 0$ para todo $i = 1, \ldots, d$ e consequentemente $f = 0$.

(*iv*) Considere um ponto $a = (a_1, \ldots, a_n) \in V(\mathbb{K}[x_1, \ldots, x_n])$. Isso significa que todo polinômio de $\mathbb{K}[x_1, \ldots, x_n]$ anula a. Em particular, os polinômios $f_0(x_1, \ldots, x_n) = x_1$ e $f_1(x_1, \ldots, x_n) = x_1 - 1$ anulam a. Portanto $a_1 = 1$ e $a_1 = 0$. Isso é um absurdo.

(*v*) Considere um ponto $x \in X$. Para todo polinômio $f \in I(X)$, por definição, $f(x) = 0$. Portanto todo ponto de X é anulado por todo polinômio de $I(X)$. Isso significa que $X \subseteq V(I(X))$.

(*vi*) Considere um polinômio $f \in J$. Para todo ponto $x \in V(J)$, por definição, $f(x) = 0$. Portanto todo polinômio de J anula todo ponto de $V(J)$. Portanto $J \subseteq I(V(J))$.

(*vii*) Por construção, $I(X) \subseteq \sqrt{I(X)}$. Para mstrar a igualdade, basta mostrar que $\sqrt{I(X)} \subseteq I(X)$. Para isso, considere um polinômio $f \in \sqrt{I(X)}$. Isso significa que existe $k \in \mathbb{N}$, tal que f^k anula todos os pontos de X, ou seja, $(f(a))^k = 0$, $\forall\, a \in X$. Como $f(a) \in \mathbb{K}$ e $\mathbb{K}$ é um corpo, então $f(a) = 0$, $\forall\, a \in X$. Portanto $f \in I(X)$.

□

Considere J um ideal de $\mathbb{K}[x_1, \ldots, x_n]$. Usando as propriedades acima, obtem-se que $J \subseteq \sqrt{J} \subseteq \sqrt{I(V(J))} = I(V(J))$. Se J for um ideal radical, a primeira continência, $J \subseteq \sqrt{J}$, é uma igualdade. O teorema a seguir considera a segunda continência.

Teorema 3.1.4 (Nullstellensatz)**.** Se J é um ideal de $\mathbb{K}[x_1, \ldots, x_n]$, então $\sqrt{J} = I(V(J))$.

A seguinte afirmação é equivalente ao Nullstellensatz:

Teorema 3.1.5. Todo ideal próprio de $\mathbb{K}[x_1, \ldots, x_n]$ tem um conjunto não vazio de zeros. Em outras palavras, se I é um ideal de $\mathbb{K}[x_1, \ldots, x_n]$ e $V(I) = \emptyset$, então $I = \mathbb{K}[x_1, \ldots, x_n]$.

Demonstração da equivalência: Por um lado, usando o Nullstellensatz, se $V(J) = \emptyset$ então $\sqrt{J} = I(V(J)) = I(\emptyset) = \mathbb{K}[x_1, \ldots, x_n]$. Isso significa que se $V(J) = \emptyset$, então nenhum ideal maximal de $\mathbb{K}[x_1, \ldots, x_n]$ contém J. Consequentemente J contém estritamente todos os ideais maximais de $\mathbb{K}[x_1, \ldots, x_n]$, ou seja, $1 \in \sqrt{J}$. Portanto $1 \in J$ e $J = \mathbb{K}[x_1, \ldots, x_n]$.

Por outro lado, suponha que o único ideal $J \subseteq \mathbb{K}[x_1, \ldots, x_n]$, tal que $V(J) = \emptyset$ é $J = \mathbb{K}[x_1, \ldots, x_n]$. Como $\mathbb{K}[x_1, \ldots, x_n]$ é noetheriano, existem $f_1, \ldots, f_k \in \mathbb{K}[x_1, \ldots, x_n]$, tais que $J = \langle f_1, \ldots, f_k \rangle$. Considere $f \in I(V(J))$ e defina $\widetilde{J}$ como o ideal

$$\widetilde{J} = \langle (1 - x_0 f), f_1, \ldots, f_k \rangle \subseteq \mathbb{K}[x_0, x_1, \ldots, x_n].$$

Se $a \in V(\widetilde{J}) \subseteq \mathbb{A}^{n+1}$, então $a_0 f(a) - 1 = 0$ e $f_i(a) = 0$ para todo $i = 1, \ldots, k$. Isso é uma contradição, pois se $a_0 f(a) - 1 = 0$, então $f(a) \neq 0$ e $a \notin V(\widetilde{J})$. Logo $V(\widetilde{J}) = \emptyset$. Usando a afirmação do teorema, $\widetilde{J} = \langle 1 \rangle$. Por isso, existem $h_0, h_1, \ldots, h_k \in \mathbb{K}[x_0, x_1, \ldots, x_n]$, tais que

$$h_0(1 - f x_0) + h_1 f_1 + \ldots + h_k f_k = 1.$$

Restringindo-se a $V(\langle x_0 f - 1 \rangle)$, temos que $h_1 f_1 + \ldots + h_k f_k = 1$, onde $h_i \in \mathbb{K}[1/f, x_1, \ldots, x_n]$, $\forall\ i = 1, \ldots, k$, e tomando $l \in \mathbb{N}$ suficientemente grande, existem polinômios $\widetilde{h}_0, \widetilde{h}_1, \ldots, \widetilde{h}_k \in \mathbb{K}[x_1, \ldots, x_n]$, $\widetilde{h}_i = h_i f^l$, $\forall\ i = 1, \ldots, k$, tais que $\widetilde{h}_1 f_1 + \ldots + \widetilde{h}_k f_k = f^l$. Isso significa que, para todo $f \in I(V(J)) \subseteq \mathbb{K}[x_1, \ldots, x_n]$, existe $l \in \mathbb{N}$, tal que $f^l \in \langle f_1, \ldots, f_k \rangle = J$. Ou seja, $I(V(J)) \subseteq \sqrt{J}$. $\square$

Demonstração do teorema: Para provar que $V(I) = \emptyset$ implica $I = \mathbb{K}[x_1, \ldots, x_n]$, considere $\mathfrak{m}$ um ideal maximal de $\mathbb{K}[x_1, \ldots, x_n]$ contendo I. Como $\mathfrak{m}$ é maximal, $\mathbb{K}[x_1, \ldots, x_n]/\mathfrak{m}$ é um corpo e além disso estende $\mathbb{K}$ algebricamente. Como $\mathbb{K}$ é algebricamente fechado, existe um morfismo de anéis $\varphi : \mathbb{K}[x_1, \ldots, x_n]/\mathfrak{m} \xrightarrow{\simeq} \mathbb{K}$. Consequentemente $\mathfrak{m}$ é da forma $\mathfrak{m}_a = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$, onde $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$ e $a \in V(\mathfrak{m}) \subseteq V(I)$. Portanto $V(I) \neq \emptyset$. $\square$

Estas duas formulações do Nullstellensatz têm consequências importantes.

Corolário 3.1.6.

(i) Existe uma bijeção entre os ideais radicais de $\mathbb{K}[x_1, \ldots, x_n]$ e as variedades afins de $\mathbb{A}^n$.

Dem: Explicitamente, a bijeção é a seguinte. Para cada ideal radical $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ associe a variedade $V(I)$ e a cada variedade $X \subseteq \mathbb{A}^n$ associe o ideal $I(X)$. $\square$

(ii) Existe uma bijeção entre os ideais maximais de $\mathbb{K}[x_1, \ldots, x_n]$ e os pontos de $\mathbb{A}^n$.

Dem: De fato, se A é uma $\mathbb{K}$-álgebra finitamente gerada e $\mathfrak{m}$ é um ideal maximal de A, então $A/\mathfrak{m}$ é um corpo que estende $\mathbb{K}$ algebricamente. Como $\mathbb{K}$ é algebricamente fechado, $A/\mathfrak{m}$ tem que ser o próprio corpo $\mathbb{K}$. Considere $A = \mathbb{K}[x_1, \ldots, x_n]$. Como a imagem de todos os polinômios de $\mathbb{K}[x_1, \ldots, x_n]$ através do morfismo quociente : $\mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}[x_1, \ldots, x_n]/\mathfrak{m} \xrightarrow{\simeq} \mathbb{K}$ são identificados com elementos de $\mathbb{K}$, a imagem de cada polinômio da forma $x_i \in \mathbb{K}[x_1, \ldots, x_n]$ é identificado com um $a_i \in \mathbb{K}$. Portanto para todo ideal maximal $\mathfrak{m} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ existe $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$, tal que $\mathfrak{m}$ contém um ideal da forma $\mathfrak{m}_a = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Como esses ideais $\mathfrak{m}_a$ são maximais, todo ideal maximal é da forma $\mathfrak{m}_a$, $a \in \mathbb{A}^n$. Portanto, a bijeção entre os ideais maximais de $\mathbb{K}[x_1, \ldots, x_n]$ e os pontos de $\mathbb{A}^n$ é dada por : $a \mapsto \mathfrak{m}_a$. $\square$

Até agora, o espaço afim n-dimensional foi considerado apenas como um conjunto. A seguinte proposição permite muní-lo de uma topologia.

Proposição 3.1.7.

(i) $\emptyset = V(\mathbb{K}[x_1, \ldots, x_n])$ e $\mathbb{A}^n = V(0)$ para todo $n \in \mathbb{N}^\bullet$.

(ii) A interseção de variedades afins é uma variedade afim.

(iii) A união finita de variedades afins é uma variedade afim.

Dem: (i) Óbvio.

(ii) Seja $\{I_j\}_j$ uma família de ideais de $\mathbb{K}[x_1, \ldots, x_n]$. Vamos mostrar que

$$\bigcap_j V(I_j) = V\left(\sum_j I_j\right).$$

Um ponto x pertence a $\bigcap_j V(I_j)$ se, e somente se, $x \in V(I_j)$ para todo j. Isso significa que todo polinômio em I_j, para todo j, anula x. Portanto todo polinômio em $\bigcup_j I_j$ anula x. Ou seja, $x \in V\left(\sum_j I_j\right)$.

(iii) Sejam $I_1, \ldots, I_m$ ideais de $\mathbb{K}[x_1, \ldots, x_n]$. Vamos mostrar que

$$\bigcup_{k=1}^{m} V(I_k) = V\left(\bigcap_{k=1}^{m} I_k\right).$$

Um ponto x pertence a $\bigcup_{k=1}^m V(I_k)$ se, e somente se, $x \in V(I_k)$ para algum $k = 1, \ldots, m$. Isso significa que x é anulado por todos os polinômios de I_k para algum $k = 1, \ldots, m$. Por um lado, x é anulado por todos os polinômios de $\bigcap_{k=1}^m I_k$, porque $\bigcap_{k=1}^m I_k \subseteq I_k$, $\forall\ k = 1, \ldots, m$. Por outro lado, se $x \in V\left(\bigcap_{k=1}^m I_k\right)$, então $x \in V\left(I_1 \ldots I_m\right)$, porque $I_1 \ldots I_m \subseteq \bigcap_{k=1}^m I_k$. Consequentemente $x \in V(I_k)$ para algum $k = 1, \ldots, m$. Caso contrário, tome $f_1 \in I_1, \ldots, f_m \in I_m$, tais que $f_k(x) \neq 0$, $\forall\ k = 1, \ldots, m$. Então $f_1 \ldots f_m \in I_1 \ldots I_m$, mas $f_1 \ldots f_m(x) \neq 0$, o que é um absurdo.

□

Definição 3.1.8. Defina os subconjuntos fechados de $\mathbb{A}^n$ como as variedades afins, ou seja, os conjuntos da forma $X = V(I)$ para algum ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$.

Pela proposição 3.1.7, a definição 3.1.8 mune o espaço afim de uma topologia. Esta topologia é chamada de *topologia de Zariski* no espaço afim.

Usando o fato de que o anel de polinômios é um anel noetheriano, todo ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ pode ser escrito como $I = \langle f_1, \ldots, f_m \rangle$, $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$. Consequentemente toda variedade afim $X \subseteq \mathbb{A}^n$ pode ser escrita como $X = V(\langle f_1, \ldots, f_m \rangle)$. Pela proposição 3.1.7, $V(\langle f_1, \ldots, f_m \rangle)$ é interseção de um conjunto finito de variedades afins, a saber, $\{V(\langle f_i \rangle) \mid i = 1, \ldots, m\}$.

Como todo subconjunto fechado de $\mathbb{A}^n$ pode ser escrito como interseção finita de variedades da forma $V(\langle f \rangle)$, onde $f \in \mathbb{K}[x_1, \ldots, x_n]$, todo aberto de $\mathbb{A}^n$ pode ser escrito como união finita de abertos da forma $V(\langle f\rangle)^c$. Consequentemente esses abertos definidos como complementares dos zeros de um ideal principal formam uma base para a topologia de Zariski no espaço afim. Além disso, os abertos de $\mathbb{A}^n$ são gerados como uniões finitas desses abertos básicos, ou seja, $\mathbb{A}^n$ satisfaz a condição de cadeias ascendentes em abertos.

Definição 3.1.9. Seja $\mathbb{A}^n$ um espaço afim. Para todo $f \in \mathbb{K}[x_1, \ldots, x_n]$, defina $D(f) = V(\langle f\rangle)^c$. Os abertos da forma $D(f)$, $f \in \mathbb{K}[x_1, \ldots, x_n]$, são chamados de *abertos principais* de $\mathbb{A}^n$.

Um espaço topológico que satisfaz a condição de cadeias ascendentes em abertos é chamado de *noetheriano*.

Exemplo 3.1.10. Algumas variedades afins e alguns abertos principais importantes:

(i) Para todo $n \in \mathbb{N}^\bullet$, $\mathbb{A}^n$ é uma variedade afim.

(ii) Considere o subconjunto $(\mathbb{A}^1)^\bullet \subseteq \mathbb{A}^1$. Esse subconjunto é um aberto principal. De fato, $(\mathbb{A}^1)^\bullet = D(x)$, $x \in \mathbb{K}[x]$.

(iii) Considere um $\mathbb{K}$-espaço vetorial V. O conjunto de transformações lineares inversíveis de V para V é denotado por $Gl(V)$. Se V tem dimensão finita, $\dim V = n$, é possível identificar $Gl(V)$ com o conjunto de matrizes inversíveis de ordem n e entradas em $\mathbb{K}$. Esse conjunto é chamado de *grupo linear geral* e é denotado por $Gl_n(\mathbb{K})$. Tais matrizes são as matrizes de ordem n cujo determinante é não nulo. Como o grupo linear geral é o conjunto de matrizes complementar ao conjunto de zeros da função determinante e o determinante é uma função polinomial nas entradas da matriz, a saber,

$$\det(x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}) = \sum_{\sigma \in S_n} (-1)^\sigma x_{1\sigma(1)} x_{2\sigma(2)} \ldots x_{n\sigma(n)},$$

esse conjunto é um aberto principal no espaço afim $\mathbb{A}^{n^2}$.

(iv) Considere o conjunto de matrizes $A \in Gl_n(\mathbb{K})$ cujo determinante é 1. Esse conjunto é chamado de *grupo linear especial* e é denotado por $Sl_n(\mathbb{K})$. Usando de novo o fato do determinante ser uma função polinomial nas entradas da matriz A, esse conjunto é uma variedade afim em $\mathbb{A}^{n^2}$. De fato, $Sl_n(\mathbb{K}) = V(\langle \det(x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}) - 1\rangle)$.

(v) Seja $\mathbb{K}$ um corpo de característica diferente de 2. Considere o conjunto de matrizes $A \in Gl_{2n}(\mathbb{K})$, tais que

$$A^t \begin{pmatrix} 0 & J \\ -J & 0 \end{pmatrix} A = \begin{pmatrix} 0 & J \\ -J & 0 \end{pmatrix}, \text{ onde } J = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}. \tag{3.1.1}$$

Esse conjunto é chamado de *grupo simplético* e é denotado por $Sp_{2n}(\mathbb{K})$. Tal conjunto é uma variedade afim do espaço $\mathbb{A}^{4n^2}$. O ideal associado a esta variedade é dado por polinômios nas entradas da matriz A provenientes da igualdade 3.1.1.

(vi) Seja $\mathbb{K}$ um corpo de característica diferente de 2. Considere o conjunto de matrizes $A \in Gl_n(\mathbb{K})$, tais que $A^t\widetilde{J}A = \widetilde{J}$, onde

$$\widetilde{J} = \begin{pmatrix} 0 & J \\ J & 0 \end{pmatrix}, \text{ no caso em que } n = 2k$$
$$\widetilde{J} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & J \\ 0 & J & 0 \end{pmatrix}, \text{ no caso em que } n = 2k-1, k \in \mathbb{N}^\bullet.$$

Esse conjunto é chamado de *grupo ortogonal* e é denotado por $O_n(\mathbb{K})$. Tal conjunto é uma variedade afim do espaço $\mathbb{A}^{n^2}$. O ideal associado a esta variedade é dado por polinômios nas entradas da matriz A provenientes da equação $A^t\widetilde{J}A = \widetilde{J}$.

(vii) As matrizes triangulares superiores de ordem n também formam uma variedade afim. Esta variedade é denotada por $T_n(\mathbb{K})$ e é o zero do ideal de polinômios

$$\langle x_{ij} : n \geq i > j \geq 1 \rangle \subseteq \mathbb{K}[x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}].$$

(viii) As matrizes triangulares superiores de ordem n com os elementos da diagonal iguais a 1 formam uma variedade afim. Esta variedade é denotada por $U_n(\mathbb{K})$ e é definida como $V(\langle x_{ij}, x_{kk} - 1 : n \geq i > j \geq 1, k = 1, \ldots, n\rangle) \subseteq \mathbb{A}^n$.

(ix) As matrizes diagonais de ordem n formam uma variedade afim. Esta variedade é denotada por $D_n(\mathbb{K})$ e é definida como $V(\langle x_{ij} : i \neq j\rangle) \subseteq \mathbb{A}^n$.

Definição 3.1.11. Um espaço topológico não vazio X é chamado de *irredutível* quando não for possível escrevê-lo como união de dois subconjuntos fechados próprios. Ou seja, se F_1, F_2 são dois fechados próprios de X, então $F_1 \cup F_2 \subsetneq X$. (Observe que não se pede que a união seja disjunta.)

Proposição 3.1.12.

(i) Um espaço topológico é irredutível se, e somente se, quaisquer dois abertos não vazios se intersectam.

(ii) O espaço afim com a topologia de Zariski é irredutível.

(iii) Um subespaço de um espaço topológico é irredutível (com a topologia induzida) se, e somente se, o seu fecho também é irredutível.

(iv) A imagem de um espaço irredutível por uma função contínua é irredutível.

Dem: *(i)* Por definição, um espaço topológico X é irredutível se e somente se $F_1 \cup F_2 \subsetneq X$ para quaisquer F_1, F_2 fechados próprios de X. Portanto, para quaisquer dois abertos não vazios, $A_1, A_2 \subseteq X$, $A_1 \cap A_2 = (A_1^c \cup A_2^c)^c \supsetneq X^c = \emptyset$.

(ii) Considere F um subconjunto fechado de $\mathbb{A}^n$. Como F é fechado, $F = V(I)$ para algum ideal $I = \langle f_1, \ldots, f_k\rangle$, $f_1, \ldots, f_k \in \mathbb{K}[x_1 \ldots, x_n]$. Consequentemente, $F = V(\langle f_1\rangle) \cap$

$\ldots \cap V(\langle f_k \rangle)$. Se $F' \subseteq \mathbb{A}^n$ é outro fechado, então existem $f'_1, \ldots, f'_l \in \mathbb{K}[x_1 \ldots, x_n]$, tais que $F' = V(\langle f'_1 \rangle) \cap \ldots \cap V(\langle f'_l \rangle)$. Portanto

$$F \cup F' = \cap_{i,j} V(\langle f_i \rangle) \cup V(\langle f'_j \rangle) = \cap_{i,j} V(\langle f_i f'_j \rangle).$$

Isso implica que $F \cup F' = \mathbb{A}^n$ se, e somente se $V(\langle f_i f'_j \rangle) = \mathbb{A}^n$ para todo f_i, f'_j, $i = 1, \ldots, k$ e $j = 1, \ldots, l$. Usando o Nullstellensatz, contanto que f_i, f'_j sejam não nulos, isso é um absurdo.

(iii) Por um lado, seja Y um subespaço de X, tal que $\overline{Y}$ é redutível. Existem $Y_1, Y_2 \subseteq \overline{Y}$, tais que Y_1, Y_2 são fechados próprios e $Y_1 \cup Y_2 = \overline{Y}$. Com a topologia induzida $(Y \cap Y_1) \cup (Y \cap Y_2) = Y$ é uma decomposição de Y em fechados próprios. Portanto Y é redutível.

Por outro lado, se Y for redutível, então $Y = Y_1 \cup Y_2$ e $\overline{Y} = \overline{Y_1} \cup \overline{Y_2}$. Portanto $\overline{Y}$ também é redutível.

(iv) Seja $\varphi : X \to Y$ uma função contínua e sobrejetora com Y redutível, $Y = Y_1 \cup Y_2$. Então $\varphi^{-1}(Y) = X = \varphi^{-1}(Y_1) \cup \varphi^{-1}(Y_2)$. Como φ é contínua, $\varphi^{-1}(Y_1), \varphi^{-1}(Y_2)$ são fechados e X é redutível.

□

Exemplo 3.1.13.

(i) Como já foi visto, o espaço afim $\mathbb{A}^2$ é irredutível. No entanto, a variedade afim $V(\langle xy \rangle)$ é redutível. De fato, $V(\langle xy \rangle) = V(\langle x \rangle) \cup V(\langle y \rangle)$.

(ii) Os espaços $(\mathbb{A}^1)^\bullet$, $Gl_n(\mathbb{K})$, $Sl_n(\mathbb{K})$, $T_n(\mathbb{K})$, $U_n(\mathbb{K})$ e $D_n(\mathbb{K})$ são irredutíveis.

Teorema 3.1.14. Todo espaço topológico noetheriano pode ser decomposto como união finita de subespaços irredutíveis maximais (portanto fechados).

Dem: Seja X um espaço topológico noetheriano. Suponha que X não seja irredutível nem possa ser decomposto como união finita de fechados irredutíveis. Considere $\mathtt{C}$ a coleção não vazia de subconjuntos fechados de X que não podem ser escritos como união finita de componentes irredutíveis. Usando o fato de X ser noetheriano, existe um elemento minimal nesta coleção. Ou seja, existe um subconjunto fechado $Y_0 \subseteq X$ que não pode ser decomposto como união finita de subconjuntos fechados e irredutíves de X, tal que, para todo conjunto $Y \in \mathtt{C}$, se $Y \subseteq Y_0$, então $Y = Y_0$. Se Y_0 fosse irredutível, então Y_0 seria trivialmente decomposto como união finita de subconjuntos irredutíveis de X, portanto Y_0 é redutível. Decomponha Y_0 em $Y_0 = Y_1 \cup Y_2$, de tal forma que $Y_1, Y_2 \subseteq Y$ e Y_1, Y_2 ou estão em $\mathtt{C}$ ou são irredutíveis. Se Y_1 e Y_2 forem irredutíveis, então Y_0 não pode pertencer a $\mathtt{C}$. Se Y_1 e Y_2 pertencerem a $\mathtt{C}$, então Y_0 não seria minimal em $\mathtt{C}$. Portanto o fato de X não poder ser decomposto como união finita de componentes irredutíveis é um absurdo.

Considere uma decomposição de X como união finita de subconjuntos fechados irredutíveis, $X = X_1 \cup \ldots \cup X_k$. Considere ainda $Y \subseteq X$ um subconjunto fechado irredutível maximal. Intersectando Y com X obtem-se uma decomposição de Y em componentes irredutíveis fechadas $Y = (Y \cap X_1) \cup \ldots \cup (Y \cap X_k)$. No entanto o fato de Y ser irredutível implica que $Y \subseteq X_i$ para algum $i = 1, \ldots, k$. Como Y é uma componente irredutível maximal, $Y = X_i$, ou seja, X_i é uma componente irredutível maximal e $X = X_1 \cup \ldots \cup X_k$ é uma decomposição de X em componentes irredutíveis maximais. □

Corolário 3.1.15. Uma variedade afim $X \subseteq \mathbb{A}^n$ é irredutível se, e somente se, $I(X)$ é um ideal primo de $\mathbb{K}[x_1, \ldots, x_n]$.

Dem: Se $I(X)$ for primo, então X é irredutível. Caso contrário, existe uma decomposição própria $X = X_1 \cup X_2$. Usando a propriedade 3.1.7,

$$I(X) = I(X_1 \cup X_2) = I(X_1) \cap I(X_2).$$

Portanto existem $f_1 \in I(X_1) \setminus I(X_2)$ e $f_2 \in I(X_2) \setminus I(X_1)$, tais que $f_1, f_2 \notin I(X)$. No entanto $f_1 f_2 \in I(X_1) \cap I(X_2) = I(X)$. Como $I(X)$ é primo, isso é um absurdo.

Suponha que X seja irredutível. Considere $fg \in I(X)$, $f, g \in \mathbb{K}[x_1, \ldots, x_n]$. Como $fg \in I(X)$, pela proposição 3.1.7, $X \subseteq V(\langle f \rangle) \cup V(\langle g \rangle)$. Considere então a decomposição $X = (X \cap V(\langle f \rangle)) \cup (X \cap V(\langle g \rangle))$. Como X é irredutível, $X \subseteq V(\langle g \rangle)$ ou $X \subseteq V(\langle f \rangle)$. Ou seja, ou $f \in I(X)$ ou $g \in I(X)$. Conclusão: $I(X)$ é primo. $\square$

A seguinte proposição trata da topologia do produto de espaços afins.

Proposição 3.1.16. Sejam $X \subset \mathbb{A}^n$ e $Y \subset \mathbb{A}^m$ duas variedades afins irredutíveis. Então $X \times Y$ munida da topologia induzida de $\mathbb{A}^{n+m}$ é uma variedade afim irredutível.

3.1.2 Morfismos afins

Definição 3.1.17. Seja $X \subseteq \mathbb{A}^n$ uma variedade afim. Define-se uma *função regular* em X como uma função $f : X \to \mathbb{A}^1$ para a qual existe $\varphi \in \mathbb{K}[x_1, \ldots, x_n]$, tal que $f(x) = \varphi(x)$ para todo $x \in X$.

Essencialmente as funções regulares de uma variedade afim são polinômios restritos a esta variedade. Portanto estas funções regulares podem ser munidos de uma estrutura de álgebra análoga à da álgebra de polinômios. Explicitamente, dadas f, g duas funções regulares numa variedade afim X, para cada $x \in X$:

(i) $(f + g)(x) = f(x) + g(x)$,

(ii) $(fg)(x) = f(x)g(x)$,

(iii) Para cada $k \in \mathbb{K}$, $(kf)(x) = kf(x)$.

Definição 3.1.18. Seja $X \subseteq \mathbb{A}^n$ uma variedade afim. Define-se o *anel de funções regulares* de X como o conjunto de funções regulares nesta variedade munido das operações descritas acima. O anel de funções regulares também é chamado de *álgebra de funções regulares*, ou *álgebra afim*, ou *anel de coordenadas* da variedade X e é denotado por $\mathbb{K}[X]$.

Considere uma variedade afim X. Como as funções regulares $\mathbb{K}[X]$ são, essencialmente, polinômios restritos a variedade X, duas funções $f, g \in \mathbb{K}[X]$ são iguais se $f - g$ for não nula somente em pontos fora de X. Ou seja, se $\langle f - g \rangle \subseteq I(X)$, então f e g serão a mesma função regular em X. Isso justifica a seguinte proposição.

Proposição 3.1.19. Seja $X \subseteq \mathbb{A}^n$ uma variedade afim. O anel de funções regulares $\mathbb{K}[X]$ é isomorfo a $\mathbb{K}[x_1, \ldots, x_n]/I(X)$.

Exemplo 3.1.20. Alguns anéis de funções regulares:

(i) O anel de funções regulares dos espaços afins são $\mathbb{K}[\mathbb{A}^n] \simeq \mathbb{K}[x_1, \ldots, x_n]$ para cada $n \in \mathbb{N}^\bullet$.

(ii) Considere o ideal de polinômios $I = \langle xy - 1 \rangle \subseteq \mathbb{K}[x, y]$. A variedade afim associada a esse ideal é $X = \{(x, y) \in \mathbb{A}^2 \mid y = 1/x,\ x \in \mathbb{K}^\bullet\}$. Seu anel de funções regulares é $\mathbb{K}[X] \simeq \mathbb{K}[x, x^{-1}]$.

(iii) Considere o anel de polinômios $\mathbb{K}[x_0, x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}]$ e o ideal de polinômios

$$I = \langle x_0 \det -1 \rangle \subseteq \mathbb{K}[x_0, x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}],$$

onde det é o polinômio determinante. A variedade afim associada a esse ideal é

$$X = \{(x_0, x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}) \in \mathbb{A}^{n^2+1} \mid \det = 1/x_0,\ x_0 \in \mathbb{K}^\bullet\}.$$

O anel de funções regulares de X é isomorfo ao anel $\mathbb{K}[x_{11}, x_{12}, \ldots, x_{n,n-1}, x_{nn}, 1/\det]$.

(iv) O anel de funções regulares de $Sl_n(\mathbb{K})$ é dado por $\mathbb{K}[x_{11}, x_{12}, \ldots, x_{n,n-1}, x_{nn}]/I$, onde $I = \langle \det -1 \rangle$.

(v) O anel de funções regulares de $T_n(\mathbb{K})$ (exemplo 3.1.10 (vii)) é dado pelo quociente do anel $\mathbb{K}[x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}]$ pelo ideal $\langle x_{ij} : 1 \leq j < i \leq n \rangle$. Portanto $\mathbb{K}[T_n]$ é isomorfo a $\mathbb{K}[x_{ij} : 1 \leq i \leq j \leq n]$.

(vi) O anel de funções regulares de $U_n(\mathbb{K})$ (exemplo 3.1.10 ($viii$)) é dado pelo quociente do anel $\mathbb{K}[x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}]$ pelo ideal $\langle x_{ij}, (x_{kk} - 1) : 1 \leq j < i \leq n,\ k = 1, \ldots, n \rangle$. Portanto $\mathbb{K}[U_n] \simeq \mathbb{K}[x_{ij} : 1 \leq i < j \leq n]$.

(vii) O anel de funções regulares de $D_n(\mathbb{K})$ (exemplo 3.1.10 (ix)) é dado pelo quociente do anel $\mathbb{K}[x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}]$ pelo ideal $\langle x_{ij} : 1 \leq i \neq j \leq n \rangle$. Então $D_n(\mathbb{K}) \simeq \mathbb{K}[x_{11}, x_{22}, \ldots, x_{nn}] \simeq \mathbb{K}[\mathbb{A}^n]$.

Proposição 3.1.21. O anel de funções regulares de uma variedade afim é uma $\mathbb{K}$-álgebra finitamente gerada e reduzida (ou seja, não tem elementos nilpotentes).

Dem: Seja $X \subseteq \mathbb{A}^n$ uma variedade afim. Pela proposição anterior, o seu anel de funções regulares é isomorfo a $\mathbb{K}[x_1, \ldots, x_n]/I(X)$. Portanto $\mathbb{K}[X]$ é uma $\mathbb{K}$-álgebra finitamente gerada pelas imagens de $x_1, \ldots, x_n$ através do morfismo

$$\mathbb{K}[x_1 \ldots, x_n] \to \mathbb{K}[x_1 \ldots, x_n]/I(X) \xrightarrow{\simeq} \mathbb{K}[X].$$

Usando o Nullstellensatz, obtem-se que $I(X)$ é radical e portanto $\mathbb{K}[x_1, \ldots, x_n]/I(X)$ é reduzida. Como $\mathbb{K}[X]$ é isomorfa a $\mathbb{K}[x_1, \ldots, x_n]/I(X)$, conclui-se que $\mathbb{K}[X]$ é finitamente gerada e reduzida. $\square$

É usual, em matemática, aplicar o seguinte processo. Dada uma definição, procura-se as propriedades satisfeitas pelos objetos que se encaixam nesta definição. Dadas algumas destas propriedades, axiomatiza-se-as, abstraindo-se dos objetos que satisfazem a definição inicial. Por fim, procura-se os objetos que satisfazem esses axiomas e compara-se esses objetos com aqueles que satisfazem a definição inicial. Apliquemos esse processo.

Uma variedade afim sobre um corpo $\mathbb{K}$ é um subconjunto de um espaço afim, cujo anel de funções regulares é uma $\mathbb{K}$-álgebra finitamente gerada e reduzida. Agora, considere A uma $\mathbb{K}$-álgebra finitamente gerada e reduzida. Existe uma $\mathbb{K}$-álgebra finitamente gerada livre, a saber $\mathbb{K}[x_1, \ldots, x_n]$, da qual A é quociente. O ideal que quocienta esta $\mathbb{K}$-álgebra livre tem que ser radical, pois A é reduzida. Esse ideal é o ideal associado a uma variedade afim cujo anel de funções regulares é A.

Esta associação entre variedades afins e álgebras finitamente geradas e reduzidas é bem estreita. Em particular, pelo Nullstellensatz, os pontos de uma variedade afim $X \subseteq \mathbb{A}^n$ são associados aos ideais maximais do anel de funções regulares $\mathbb{K}[X]$. Esses ideais são os ideais maximais da álgebra finitamente gerada livre $\mathbb{K}[\mathbb{A}^n]$ que contêm o ideal associado a variedade afim $I(X)$.

Dada a definição de função regular, é natural se perguntar por seu análogo para um espaço afim de dimensão n ou para uma outra variedade afim.

Definição 3.1.22. Um *morfismo de espaços afins* é uma função $f : \mathbb{A}^n \to \mathbb{A}^m$ entre dois espaços afins, $f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$, tal que cada componente f_i, $i = 1, \ldots, m$, é uma função regular de $\mathbb{A}^n$.

Sejam $X \subseteq \mathbb{A}^n$ e $Y \subseteq \mathbb{A}^m$ duas variedades afins. Uma função $f : X \to Y$, $f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$, é um *morfismo de variedades afins* quando cada componente f_i, $i = 1, \ldots, m$, é uma função regular de X.

Exemplo 3.1.23.

(i) Considere a variedade $X = V(\langle xy - 1\rangle) \subseteq \mathbb{A}^2$ (do exemplo 3.1.20) e o aberto principal $(\mathbb{A}^1)^\bullet \subseteq \mathbb{A}^1$. Considere a função $\varphi : X \to \mathbb{A}^1$ definida por $\varphi(x, y) = x$. Esta função é um morfismo de variedades pois é polinomial. Além disso, φ é uma bijeção entre X e $(\mathbb{A}^1)^\bullet$. Ou seja, φ é um isomorfismo entre $V(\langle xy - 1\rangle)$ e $(\mathbb{A}^1)^\bullet$.

(ii) Considere a variedade $Y = V(\langle x_0 \det -1\rangle) \subseteq \mathbb{A}^{n^2+1}$ (do exemplo 3.1.20) e o aberto principal $Gl_n(\mathbb{K}) \subseteq \mathbb{A}^{n^2}$. Considere a função $\varphi : Y \to \mathbb{A}^{n^2}$ definida por $\varphi(x_0, x_{11}, \ldots, x_{nn}) = (x_{11}, \ldots, x_{nn})$. Esta função é um morfismo por ser polinômial. Além disso φ é uma bijeção entre Y e $Gl_n(\mathbb{K})$. Portanto φ é um isomorfismo entre $V(\langle x_0 \det -1\rangle)$ e $Gl_n(\mathbb{K})$.

Proposição 3.1.24. Sejam $X \subseteq \mathbb{A}^n$ e $Y \subseteq \mathbb{A}^m$ duas variedades afins. Uma função $\varphi : X \to Y$ é um *morfismo de variedades afins* se, e somente se, $g \circ \varphi \in \mathbb{K}[X]$, $\forall\, g \in \mathbb{K}[Y]$.

Dem: Se φ for um morfismo de variedades afins, então existem $\varphi_1, \ldots, \varphi_m \in \mathbb{K}[x_1, \ldots, x_n]$, tais que $\varphi(x_1, \ldots, x_n) = (\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_m(x_1, \ldots, x_n))$ para todo $(x_1, \ldots, x_n) \in X$. Como g é uma função regular em Y, existe $\psi \in \mathbb{K}[x_1, \ldots, x_m]$, tal que $g(y) = \psi(y)$ para todo $y \in Y$. Portanto $g \circ \varphi$ pode ser escrita como $\psi \circ (\varphi_1, \ldots, \varphi_m)$. Isso implica que $g \circ \varphi$ é uma função regular em X para todo $g \in \mathbb{K}[Y]$.

Por outro lado, se $g \circ \varphi$ for uma função regular para todo $g \in \mathbb{K}[Y]$, então, em particular, $x_i \circ \varphi = \varphi_i$ é regular para todo $i = 1, \ldots, m$. Isso significa que φ é um morfismo de variedades afins. $\square$

A proposição anterior motiva a seguinte definição.

Definição 3.1.25. Seja $\varphi : X \to Y$ um morfismo entre variedades afins. Define-se o *comorfismo* φ^* como o morfismo de $\mathbb{K}$-álgebras $\varphi^* : \mathbb{K}[Y] \to \mathbb{K}[X]$ tal que, para cada $g \in \mathbb{K}[Y]$, $\varphi^*(g) = g \circ \varphi$.

Proposição 3.1.26. Sejam X e Y duas variedades afins:

(*i*) Se a imagem de um morfismo $\varphi : X \to Y$ é densa em Y, então o comorfismo $\varphi^* : \mathbb{K}[Y] \to \mathbb{K}[X]$ é injetor.

(*ii*) $\mathbb{K}[X \times Y] \simeq \mathbb{K}[X] \otimes_{\mathbb{K}} \mathbb{K}[Y]$.

Dem: (*i*) Suponha que a imagem de φ seja densa em Y e que existam $f, g \in \mathbb{K}[Y]$, tais que $\varphi^*(f) = \varphi^*(g)$. Isso significa que $f \circ \varphi(x) = g \circ \varphi(x)$ para todo $x \in X$. Como a imagem de φ é densa em Y e f, g são contínuas, $f(y) = g(y)$ para todo $y \in Y$. Nesse caso, $f = g$ e portanto φ^* é injetiva.

(*ii*) Considere a função $\psi : \mathbb{K}[X] \otimes_{\mathbb{K}} \mathbb{K}[Y] \to \mathbb{K}[X \times Y]$, tal que $\psi(f \otimes g)(x, y) = f(x)g(y)$ para cada $f \in \mathbb{K}[X]$, $g \in \mathbb{K}[Y]$, $x \in X$ e $y \in Y$.

Esta função é bilinear e portanto estende para um morfismo de álgebras q denotaremos pelo mesmo símbolo $\psi : \mathbb{K}[X] \otimes_{\mathbb{K}} \mathbb{K}[Y] \to \mathbb{K}[X \times Y]$. Para mostrar o isomorfismo, basta verificar que ψ é bijetora.

A sobrejetividade é clara a partir do fato de todas as variáveis do anel de coordenadas $\mathbb{K}[X \times Y]$ poderem ser escritas como combinações algébricas de f e g.

Para provar que ψ é injetora, considere $f = \sum_i g_i \otimes h_i$, tal que $\psi(f) = 0$. Sem perda de generalidade assuma que $f = \sum_{i=1}^{k} g_i \otimes h_i$ é escrita com k minimal. Se $f \neq 0$, nem todo h_i pode ser nulo. Considere $y_0 \in Y$, tal que $h_i(y_0) \neq 0$ para algum h_i. Como $\psi(f) = 0$, $\sum_i g_i(x)h_i(y_0) = 0$ para todo $x \in X$ e portanto $\sum_i h_i(y_0)g_i = 0$. Isso significa que o conjunto $\{g_i \mid i = 1, \ldots, k\}$ é linearmente dependente em $\mathbb{K}[X]$. Como os g_i são linearmente dependentes, é possível diminuir o número k, o que contradiz a minimalidade de k se $k > 1$. Isso implica que $k = 1$. Nesse caso, $g_1 = 0$ e portanto $f = 0$.

□

A partir da definição 3.1.22 é possível definir a categoria de variedades afins. Os objetos desta categoria são todas as variedades afins e os morfismos são os morfismos entre variedades afins. Usando a definição 3.1.25 é possível associar um morfismo de álgebras a cada morfismo de variedades afins, a saber, o comorfismo. Esta associação estende a associação feita após a proposição 3.1.21 entre as categorias de variedades afins e a categoria de $\mathbb{K}$-álgebras finitamente geradas e reduzidas. Esta associação, além de ser funtorial, é uma equivalência de categorias ([Har], seção 3, capítulo 1).

Exemplo 3.1.27. Alguns exemplos da equivalência entre categorias:

(*i*) $\mathbb{A}^n \mapsto \mathbb{K}[x_1, \ldots, x_n]$.

(*ii*) $(\mathbb{A}^1)^\bullet \mapsto \mathbb{K}[x^{-1}, x]$.

(*iii*) $Gl_n(\mathbb{K}) \mapsto \mathbb{K}[x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}, 1/\det]$.

(*iv*) $Sl_n(\mathbb{K}) \mapsto \mathbb{K}[x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}]/\langle \det -1 \rangle$.

(*v*) $T_n(\mathbb{K}) \mapsto \mathbb{K}[x_{ij} : 1 \leq i \leq j \leq n]$.

(*vi*) $U_n(\mathbb{K}) \mapsto \mathbb{K}[x_{ij} : 1 \leq i < j \leq n]$.

(*vii*) $D_n(\mathbb{K}) \mapsto \mathbb{K}[x_1, \ldots, x_n]$.

Definição 3.1.28. Sejam X uma variedade afim e p um ponto de X. Uma função $f : X \to \mathbb{K}$ é dita *regular no ponto* p quando existem $U \subseteq X$ um aberto em X contendo p e $g, h \in \mathbb{K}[X]$, tais que $h(p) \neq 0$ e $f(x) = \frac{g(x)}{h(x)}$, $\forall\ x \in U$.

Proposição 3.1.29. Sejam X uma variedade afim e p um ponto de X. O conjunto de funções regulares no ponto p é um anel isomorfo à localização de $\mathbb{K}[X]$ pelo ideal maximal $I(\{p\})$.

Dem: Usando a definição acima, as funções regulares em p são as funções $f : X \to \mathbb{K}$ tais que $f(x) = \frac{g(x)}{h(x)}$, $\forall\ x \in U$, com $g, h \in \mathbb{K}[X]$ e $h(p) \neq 0$. Como X é variedade afim, existe $n \in \mathbb{N}$, tal que $X \subseteq \mathbb{A}^n$ e como $g, h \in \mathbb{K}[X]$, existem $\varphi, \psi \in \mathbb{K}[x_1, \ldots, x_n]$, tais que $\varphi(x) = g(x)$ e $\psi(x) = h(x)$ para todo $x \in U$. Isso significa que $f(x) = \frac{\varphi(x)}{\psi(x)}$ para todo $x \in U$. Observe o fato de que $\psi(p) \neq 0$. Usando esse fato e a aplicação acima que a uma função f regular em p associa $\frac{\varphi}{\psi}$, obtem-se o isomorfismo do enunciado. $\square$

A proposição anterior permite fazer a seguinte definição:

Definição 3.1.30. Sejam X uma variedade afim e x um ponto de X. Defina o *anel local de funções regulares* em x como o conjunto de todas as funções regulares no ponto x munido da estrutura de anal induzida de $\mathbb{K}[X]_{I\{x\}}$. Denote esse anel por $\mathcal{O}_{X,x}$, ou simplesmente $\mathcal{O}_x$ quando a variedade estiver subentendida.

Exemplo 3.1.31.

(*i*) O anel local de funções regulares do espaço afim $\mathbb{A}^1$ no ponto 0 é o conjunto de funções racionais $f/g \in \mathbb{K}(x)$, tais que $g(0) \neq 0$. O seu único ideal maximal é $\langle x \rangle \subseteq \mathcal{O}_{\mathbb{A}^1,0}$.

(*ii*) O anel local de funções regulares de $Gl_n(\mathbb{K})$ na identidade $e \in Gl_n(\mathbb{K})$ é o conjunto de funções racionais $f/g \in \mathbb{K}(x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn})$ tais que $g(e) \neq 0$, ou seja, $g \notin I_e = \langle x_{ij} - \delta_{ij} : 1 \leq i, j \leq n \rangle$. O único ideal maximal de $\mathcal{O}_e$ é I_e.

A próxima proposição diz que as funções regulares em toda variedade são as funções que são regulares em todos os pontos da variedade.

Proposição 3.1.32. Seja X uma variedade afim irredutível. Então $\mathbb{K}[X] \simeq \bigcap_{x \in X} \mathcal{O}_{X,x}$.

Dem: Considere $X \subseteq \mathbb{A}^n$ e uma função regular $f \in \mathbb{K}[X]$. Como existe $\psi \in \mathbb{K}[x_1, \ldots, x_n]$, tal que $f(x) = \psi(x)$ para todo $x \in X$, é possível identificar $\mathbb{K}[X]$ com o subconjunto de $\bigcap_{x \in X} \mathcal{O}_{X,x}$ que consiste das funções regulares polinomiais. Para mostrar o isomorfismo, basta mostrar agora que toda função regular em todos os pontos de X é polinomial.

Considere $f \in \bigcap_{x \in X} \mathcal{O}_{X,x}$. Isso significa que, para cada $x \in X$, existe $g_x, h_x \in \mathbb{K}[X]$ tal que $f = \frac{g_x}{h_x}$ e $h_x(x) \neq 0$. Agora considere o ideal I gerado pelo conjunto $\{h_x \mid x \in X\}$. Como $h_x(x) \neq 0$ para todo $x \in X$, não existe $x \in X$ que pertença a $V(I)$. Usando o Nullstellensatz, isso implica que $I = \langle 1 \rangle$. Portanto existem $a_i \in \mathbb{K}[X]$ tais que $1 = \sum_i a_i h_{x_i}$. Usando o fato que $f = \frac{g_{x_i}}{h_{x_i}}$ para todo $x_i \in X$, obtem-se que $f = \sum_i a_i g_{x_i}$. Isso implica que f é uma função polinomial. $\square$

Proposição 3.1.33. Sejam X e Y duas variedades afins, x um ponto de X e $\varphi : X \to Y$ um morfismo de variedades afins. Sejam $\mathfrak{m}_x$ o ideal maximal do anel local $\mathcal{O}_{X,x}$ e $\mathfrak{m}_{\varphi(x)}$ o ideal maximal do anel local $\mathcal{O}_{Y,\varphi(x)}$. Então o comorfismo $\varphi^* : \mathbb{K}[Y] \to \mathbb{K}[X]$ induz um morfismo de anéis locais $\varphi_x^* : \mathcal{O}_{Y,\varphi(x)} \to \mathcal{O}_{X,x}$ que satisfaz $\varphi_x^*(\mathfrak{m}_{\varphi(x)}) \subseteq \mathfrak{m}_x$.

Definição 3.1.34. Seja X uma variedade afim. Para todo aberto $U \subseteq X$, defina o *anel de funções regulares* em U como o conjunto de funções regulares em todo ponto do aberto U, ou seja, $\mathcal{O}_X(U) := \bigcap_{u\in U} \mathcal{O}_{X,u}$.

Observe que, segundo esta definição, $\mathcal{O}_X(X) = \mathbb{K}[X]$.

Esta definição associa abertos da variedade afim a álgebras de funções racionais, a saber os anéis de funções regulares desses abertos.

Exemplo 3.1.35.

(*i*) $\mathcal{O}_{\mathbb{A}^1}((\mathbb{A}^1)^\bullet) \simeq \mathbb{K}[x^{-1}, x]$.

(*ii*) $\mathcal{O}_{\mathbb{A}^{n^2}}(Gl_n) \simeq \mathbb{K}[x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}, 1/\det]$.

Proposição 3.1.36. Sejam X e Y duas variedades afins. Então:

(*i*) O produto $X \times Y$ é o produto na categoria de variedades afins.

(*ii*) Para todo ponto $(x, y) \in X \times Y$, o anel local $\mathcal{O}_{(x,y)}$ é a localização de $\mathcal{O}_x \otimes \mathcal{O}_y$ pelo ideal $\mathfrak{m}_x \otimes \mathcal{O}_y + \mathcal{O}_x \otimes \mathfrak{m}_y$.

Dem: (*i*) Para mostrar a propriedade de produto para $X \times Y$, considere uma variedade Z e morfismos $\psi_1 : Z \to X$ e $\psi_2 : Z \to Y$. Para construir um morfismo $\varphi : Z \to X \times Y$ que satisfaz a propriedade universal, considere a função de conjuntos que satisfaz tal propriedade (na categoria de conjuntos). É necessário provar que tal função é um morfismo de variedades afins. Usando os fatos que $\mathbb{K}[X \times Y]$ é gerado pelas imagens dos comorfismos das projeções $pr_x : X \times Y \to X$ e $pr_y : X \times Y \to Y$ e o fato de ψ_1, ψ_2 serem morfismos, obtem-se que φ é também um morfismo de variedades afins.

(*ii*) Se X e Y forem irredutíveis, então $X \times Y$ também é. Pelo item anterior, $\mathbb{K}[X] \otimes_{\mathbb{K}} \mathbb{K}[Y]$ é isomorfo a $\mathbb{K}[X \times Y]$, portanto é um domínio cujo corpo de frações é isomorfo a $\mathbb{K}(X \times Y)$. Considere as inclusões $\mathbb{K}[X] \otimes \mathbb{K}[Y] \subseteq \mathcal{O}_x \otimes \mathcal{O}_y \subseteq \mathcal{O}_{(x,y)}$. Como $\mathcal{O}_{(x,y)}$ é a localização de $\mathbb{K}[X] \otimes \mathbb{K}[Y]$ pelo ideal $\mathfrak{m}_{(x,y)}$, $\mathcal{O}_{(x,y)}$ é tam bém a localização de $\mathcal{O}_x \otimes \mathcal{O}_y$ pelo ideal $\mathfrak{m}$ que se anula em (x, y). Basta mostrar, portanto que $\mathfrak{m} = \mathfrak{m}_x \otimes \mathcal{O}_y + \mathcal{O}_x \otimes \mathfrak{m}_y$. Se $f \in \mathfrak{m}_x \otimes \mathcal{O}_y + \mathcal{O}_x \otimes \mathfrak{m}_y$, então f anula (x, y). Basta provar, portanto que $\mathfrak{m} \subseteq \mathfrak{m}_x \otimes \mathcal{O}_y + \mathcal{O}_x \otimes \mathfrak{m}_y$. Considere $f = \sum_i g_i \otimes h_i$, onde $g_i \in \mathcal{O}_x$ e $h_i \in \mathcal{O}_y$ para todo i. Considere também $g_i(x) = a_i$ e $h_i(y) = b_i$. Nesse caso, $f - \sum_i a_i b_i = \sum_i (g_i - a_i) \otimes h_i + \sum_i g_i \otimes (h_i - b_i)$ que pertence a $\mathcal{O}_x \otimes \mathfrak{m}_y + \mathfrak{m}_x \otimes \mathcal{O}_y$. Isso implica que $\sum_i a_i b_i = 0$ e portanto $f \in \mathcal{O}_x \otimes \mathfrak{m}_y + \mathfrak{m}_x \otimes \mathcal{O}_y$.

□

3.1.3 Variedades projetivas

O objetivo desta seção é descrever as variedades projetivas de maneira análoga às variedades afins. As referências para esse conteúdo são [Hum2] e [Har].

Durante esta seção, considere que $\mathbb{K}$ é um corpo algebricamente fechado.

Definição 3.1.37. Define-se uma relação de equivalência em $\mathbb{K}^{n+1^\bullet}$ da seguinte forma: $(x_0, \ldots, x_n) \cong (y_0, \ldots, y_n)$, quando $(y_0, \ldots, y_n) = (kx_0, \ldots, kx_n)$ para algum $k \in \mathbb{K}^\bullet$. Define-se o *espaço projetivo* n-dimensional $\mathbb{P}^n$ como o conjunto de classes de equivalência da relação acima.

O espaço projetivo n-dimensional pode ser visto como o espaço das retas de $\mathbb{K}^{n+1}$ que passam pela origem. Desta forma, um ponto em $\mathbb{P}^n$ pode ser representado em *coordenadas homogêneas* por $(a_0 : \ldots : a_n)$, onde $(a_0, \ldots, a_n) \in \mathbb{K}^{n+1^\bullet}$ e $(a_0 : \ldots : a_n) = (ka_0 : \ldots : ka_n)$ para todo $k \in \mathbb{K}^\bullet$.

Como as coordenadas dos pontos de $\mathbb{P}^n$ são homogêneas, não faz sentido perguntar pelo valor de um polinômio num ponto de $\mathbb{P}^n$. No entanto, faz sentido perguntar se um ponto no espaço projetivo é zero de um polinômio homogêneo ou não. De fato, quando um polinômio $f \in \mathbb{K}[x_0, \ldots, x_n]$ é homogêneo de grau d, $f(ka_0, \ldots, ka_n) = k^d f(a_0, \ldots, a_n)$ para todo $k \in \mathbb{K}^\bullet$. Nesse caso, $f(a_0, \ldots, a_n) = 0$ se, e somente se, $f(ka_0, \ldots, ka_n) = 0$, $\forall\ k \in \mathbb{K}^\bullet$.

Definição 3.1.38. Considere o conjunto de polinômios homogêneos em $\mathbb{K}[x_0, \ldots, x_n]$ e denote-o por $\mathbb{K}[x_0, \ldots, x_n]_h$. Um ideal de $\mathbb{K}[x_0, \ldots, x_n]$ é dito *homogêneo* quando for gerado por polinômios homogêneos. Para cada ideal homogêneo $I \subseteq \mathbb{K}[x_0, \ldots, x_n]$, defina a *variedade projetiva* associada a I como $V(I) = \{x \in \mathbb{P}^n \mid f(x) = 0,\ \forall\ f \in I\}$. Para cada subconjunto $X \subseteq \mathbb{P}^n$, defina o *ideal de polinômios homogêneos associado a* X, $I(X)$, como o ideal homogêneo gerado por $\{f \in \mathbb{K}[x_0, \ldots, x_n]_h \mid f(x) = 0,\ \forall\ x \in X\}$.

Proposição 3.1.39. Sejam X, Y subconjuntos de $\mathbb{P}^n$ e I, J ideais homogêneos do anel de polinômios $\mathbb{K}[x_0, \ldots, x_n]_h$.

(i) Se $Y \subseteq X$ então $I(Y) \supseteq I(X)$.

(ii) Se $I \subseteq J$ então $V(I) \supseteq V(J)$.

(iii) $I(\mathbb{P}^n) = \{0\}$ e $V(\mathbb{K}[x_0, \ldots, x_n]_h) = \emptyset$.

(iv) $X \subseteq V(I(X))$.

(v) $J \subseteq I(V(J))$.

(vi) $I(X)$ é radical em $\mathbb{K}[x_0, \ldots, x_n]_h$.

O análogo ao Nullstellensatz para o caso projetivo é:

Teorema 3.1.40. Se J é um ideal homogêneo de $\mathbb{K}[x_0, \ldots, x_n]$, tal que $\sqrt{J}$ não contém $\langle x_0, \ldots, x_n\rangle^k$, $\forall\ k \in \mathbb{N}^\bullet$, então $\sqrt{J} = I(V(J))$.

De forma equivalente:

Teorema 3.1.41. Todo ideal homogêneo de $\mathbb{K}[x_0, \ldots, x_n]$ que não contém $\langle x_0, \ldots, x_n\rangle$ tem um conjunto não vazio de zeros.

Corolário 3.1.42. Existe uma bijeção entre os fechados de $\mathbb{P}^n$ e os ideais radicais homogêneos de $\mathbb{K}[x_0, \ldots, x_n]$ diferentes de $\langle x_0, \ldots, x_n\rangle$.

Até agora, o espaço projetivo n dimensional foi considerado apenas como um conjunto. A seguinte proposição permite muní-lo de uma topologia.

Proposição 3.1.43.

(*i*) $\emptyset = V(\mathbb{K}[x_0, \ldots, x_n])$ e $\mathbb{P}^n = V(0)$.

(*ii*) A interseção de variedades projetivas é uma variedade projetiva.

(*iii*) A união finita de variedades projetivas é uma variedade projetiva.

Definição 3.1.44. Defina os subconjuntos fechados de $\mathbb{P}^n$ como as variedades projetivas, ou seja, os subconjuntos da forma $X = V(I)$ para algum ideal de polinômios homogêneos $I \subseteq \mathbb{K}[x_0, \ldots, x_n]$.

A definição acima de fato mune o espaço projetivo de uma topologia. Esta topologia é chamada de *topologia de Zariski* no espaço projetivo.

Proposição 3.1.45.

(*i*) O espaço projetivo munido da topologia de Zariski é um espaço topológico noetheriano.

(*ii*) O espaço projetivo munido da topologia de Zariski é um espaço topológico irredutível.

(*iii*) Uma variedade projetiva $X \subseteq \mathbb{P}^n$ é irredutível se, e somente se, $I(X)$ é um ideal homogêneo primo de $\mathbb{K}[x_0, \ldots, x_n]$ diferente de $\langle x_0, \ldots, x_n \rangle$.

Observe que as variedades projetivas $Y \subseteq \mathbb{P}^n$ são determinadas por ideais de polinômios em $(n+1)$ variáveis. Esses polinômios, por sua vez, determinam variedades afins $X \subseteq \mathbb{A}^{n+1}$. É natural, portanto, considerar as relações entre as variedades afins e projetivas.

Dado um polinômio $F \in \mathbb{K}[x_0, \ldots, x_n]_h$, é possível obter um polinômio em $\mathbb{K}[x_1, \ldots, x_n]$, restringindo-se ao aberto $\{(x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_0 \neq 0\} = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_0 = 1\}$. Explicitamente, seja F um polinômio homogêneo de grau d em $\mathbb{K}[x_0, \ldots, x_n]_h$. Escreva $F(x_0, \ldots x_n) = \sum_{0 \leq i \leq d} f_i(x_1, \ldots, x_n) x_0^i$, onde f_i é um polinômio homogêneo cujo grau é $(d-i)$, $\forall\ i = 0, \ldots, d$. Considere então o polinômio $f(x_1, \ldots, x_n)$ definido por $\sum_{0 \leq i \leq d} f_i(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$. Esse polinômio f é chamado de *desomogneização* de F em relação a x_0. Por construção, a variedade afim definida por f é a interseção da variedade projetiva definida por F com o aberto $\{(x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_0 \neq 0\}$.

Por outro lado, considere um polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ de grau d. Decomponha f em componentes homogêneas, $f = f_0 + \ldots + f_d$. Considere, agora, o polinômio homogêneo definido por $F(x_0, \ldots, x_n) = \sum_{0 \leq i \leq d} f_i x_0^{d-i} \in \mathbb{K}[x_0, \ldots, x_n]$. Esse polinômio F é chamado de *homogneização* de f em relação a x_0.

Agora, considere um ponto $x \in \{(x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_0 \neq 0\}$. Em coordenadas homogêneas $x = (x_0 : x_1 : \ldots : x_n) = (1 : x_1/x_0 : \ldots : x_n/x_0)$, onde $(x_1/x_0, \ldots, x_n/x_0) \in \mathbb{A}^n$. Por outro lado, todo ponto $(x_1, \ldots, x_n) \in \mathbb{A}^n$ define um único ponto $(1 : x_1 : \ldots : x_n)$ em $\{(x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_0 \neq 0\}$. Portanto existe uma bijeção entre o espaço afim $\mathbb{A}^n$ e os abertos do espaço projetivo da forma $\{(x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_i \neq 0\}$.

Definição 3.1.46. Considere $\mathbb{P}^n$ um espaço projetivo. Defina os *abertos afins* de $\mathbb{P}^n$ como os abertos $U_i = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_i \neq 0\}$, $i = 0, \ldots, n$. As coordenadas de um ponto de $\mathbb{P}^n$ num aberto afim são chamadas de *coordenadas afins*. Defina uma *variedade quasi-projetiva* como um subconjunto aberto de uma variedade projetiva.

Observe que toda variedade projetiva é uma variedade quasi-projetiva. Observe também que os abertos afins são variedades quasi-projetivas.

Proposição 3.1.47. Sejam $U_i = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_i \neq 0\}$, $i = 0, \ldots, n$, os abertos afins em $\mathbb{P}^n$. Esses abertos cobrem $\mathbb{P}^n$, ou seja, $\mathbb{P}^n = \cup_{i=0}^n U_i$. Em particular, um subconjunto é aberto ou fechado em $\mathbb{P}^n$, quando as suas intersecções com todos os abertos afins U_i, $i = 0, \ldots, n$, forem abertas ou fechadas, respectivamente.

Proposição 3.1.48. Sejam $X \subset \mathbb{P}^n$ e $Y \subset \mathbb{P}^m$ dois fechados projetivos. Defina a *aplicação de Segre* como a função $\varphi : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{(n+1)(m+1)-1}$ dada por

$$\varphi(x_0, \ldots, x_n; y_0 \ldots, y_m) = (x_0y_0 : x_0y_1 : \ldots : x_0y_m : x_1y_0 : \ldots : x_1y_m : \ldots : x_ny_0 : \ldots : x_ny_m).$$

A aplicação de Segre é uma bijeção entre $X \times Y$ e um subconjunto fechado de $\mathbb{P}^{nm+m+n}$.

3.1.4 Morfismos projetivos

Esta seção tem como objetivo expor construções análogas às feitas para as variedades afins, no caso projetivo.

Considere $\mathbb{K}$ um corpo algebricamente fechado.

Definição 3.1.49. Seja $X \subseteq \mathbb{P}^n$ uma variedade projetiva. Defina o *anel de coordenadas de* X como o anel quociente $\mathbb{K}[x_0, \ldots, x_n]/I(X)$. Denote-o por $\mathbb{K}[X]$.

Considere o espaço projetivo $\mathbb{P}^n$. Como $I(\mathbb{P}^n) = 0$, $\mathbb{K}[\mathbb{P}^n] = \mathbb{K}[x_0, \ldots, x_n]_h$.

Definição 3.1.50. Sejam $X \subseteq \mathbb{P}^n$ uma variedade projetiva e p um ponto de X. Uma função $f : X \to \mathbb{K}$ é dita *regular no ponto* p quando existem $U \subseteq X$ um aberto de X contendo p e dois polinômios homogêneos de mesmo grau, $g, h \in \mathbb{K}[X]$, tais que $h(p) \neq 0$ e $f(x) = \frac{g(x)}{h(x)}$, $\forall\ x \in u$.

Proposição 3.1.51. Sejam X uma variedade projetiva e x um ponto de X. O conjunto das funções regulares em x é o conjunto de elementos de grau zero na localização de $\mathbb{K}[X]$ pelo ideal $I(\{x\})$.

A proposição anterior permite a seguinte definição:

Definição 3.1.52. Sejam X uma variedade projetiva e x um ponto de X. Defina o *anel de funções regulares em* x como o conjunto de todas as funções regulares no ponto x. Denote esse anel local por $\mathcal{O}_{X,x}$.

Defina o *anel de funções regulares em um aberto* $U \subseteq X$ como o conjunto $\mathcal{O}_X(U)$ de funções regulares em todos os pontos de U.

Esta definição associa a cada aberto de variedade projetiva um anel, a saber, o anel de funções regulares naquele aberto. Esta construção já foi deita para variedades projetivas. Ambas são casos particulares de uma construção mais geral, o feixe.

Para todo $n \in \mathbb{N}^\bullet$, $\mathcal{O}_{\mathbb{P}^n}(\mathbb{P}^n) \simeq \mathbb{K}$. De fato, considere $f \in \mathcal{O}_{\mathbb{P}^n}(\mathbb{P}^n)$. Isso significa que existem $g, h \in \mathbb{K}[x_0, \ldots, x_n]_h$ de mesmo grau tais que $f = \frac{g}{h}$. Como f é regular em todo ponto de $\mathbb{P}^n$, h não pode ter zeros em nenhum ponto de $\mathbb{P}^n$. Isso significa que h tem grau 0. Como g tem o mesmo grau de h, o grau de g também é zero. Portanto se $f = \frac{g}{h}$ for regular em todo $\mathbb{P}^n$ então f é constante.

Definição 3.1.53. Sejam $X \subseteq \mathbb{P}^n$ e $Y \subseteq \mathbb{P}^m$ duas variedades projetivas. Um função $\varphi : X \to Y$ é dita *morfismo de variedades projetivas* quando φ for contínua e, para todo aberto $V \subseteq Y$ e toda função regular $f : V \to \mathbb{K}$, $f \circ \varphi : \varphi^{-1}(V) \to \mathbb{K}$ é uma função regular.

Proposição 3.1.54. Sejam X e Y duas variedades projetivas. Então:

(i) O produto $X \times Y$ é o produto na categoria de variedades projetivas.

(ii) $\mathbb{K}[X \times Y] \simeq \mathbb{K}[X] \otimes_{\mathbb{K}} \mathbb{K}[Y]$.

3.1.5 Feixes

O objetivo desta seção é expor um conceito que generaliza as associações entre abertos e anéis de funções regulares feitas para variedades afins e variedades projetivas. As referências são [Hum2] e [Har].

Durante esta seção, considere sempre que $\mathbb{K}$ é um corpo algebricamente fechado.

Definição 3.1.55. Seja X um espaço topológico. Diz-se que $(X, \mathcal{F}, \rho)$ é um espaço topológico munido de *pré-feixe de conjuntos* se $\mathcal{F}$ e ρ satisfazem:

(i) $\mathcal{F}$ associa a todo aberto $U \subseteq X$ um conjunto $\mathcal{F}(U)$;

(ii) $\mathcal{F}(\emptyset)$ é um conjunto formado por um ponto (que será denotado por pt);

(iii) Dados dois abertos de X, $V \subseteq U$, $\rho_V^U : \mathcal{F}(U) \to \mathcal{F}(V)$;

(iv) Para todo aberto $U \subseteq X$, $\rho_U^U = id_{\mathcal{F}(U)}$;

(v) Dados três abertos de X, $W \subseteq V \subseteq U$, $\rho_W^U = \rho_W^V \circ \rho_V^U$.

Diz-se que $(X, \mathcal{F}, \rho)$ é um espaço topológico munido de *feixe de conjuntos*, quando $\mathcal{F}$ e ρ também satisfazem:

(vi) Para todo aberto $U \subseteq X$, se $x, y \in \mathcal{F}(U)$ e $\rho_V^U(x) = \rho_V^U(y)$, para todo aberto V de uma cobertura de U, então $x = y$;

(vii) Para quaisquer abertos $U, V \subseteq X$, se $x \in \mathcal{F}(U)$, $y \in \mathcal{F}(V)$ e $\rho_{U\cap V}^U(x) = \rho_{U\cap V}^V(y)$, então existe $z \in \mathcal{F}(U \cup V)$, tal que $\rho_U^{U\cup V}(z) = x$ e $\rho_V^{U\cup V}(z) = y$.

Considere um espaço topológico X munido de um feixe de conjuntos $\mathcal{F}$ e um aberto $U \subseteq X$. Os elementos de $\mathcal{F}(U)$ são chamados de *seções locais* do feixe $\mathcal{F}$ sobre o aberto U. Analogamente, os elementos de $\mathcal{F}(X)$ são chamados de *seções globais* de $\mathcal{F}$.

A estrutura de feixe permite estudar um espaço topológico do ponto de vista local e permite globalizar informações locais. Uma variedade diferenciável real, por exemplo, pode ser vista como um espaço topológico (Hausdorff e com base enumerável para a topologia) munido de um feixe de funções com valores reais localmente isomorfo ao feixe de funções diferenciáveis em um aberto de $\mathbb{R}^n$. Nesse caso, é comum estudar a variedade olhando as cartas locais. É um papel análogo a esse que os feixes desempenham.

É possível definir feixes e pré-feixes de uma forma mais geral, como funtores.

Definição 3.1.56. Seja X um espaço topológico. Defina a categoria $Top(X)$ cujos objetos são os abertos de X e os morfismos são as restrições de abertos $\varrho^U_V : U \to V$, onde $V \subseteq U$ e U, V são abertos em X.

Seja $\mathcal{C}$ uma categoria. Um *pré-feixe em X com valores em $\mathcal{C}$* é um funtor covariante da categoria $Top(X)$ para a categoria $\mathcal{C}$. Para dois abertos $V \subseteq U \subseteq X$, denote $\mathcal{F}(\varrho^U_V)$ por ρ^U_V. Um *feixe em X* é um pré-feixe em X que satisfaz as condições 3.1.55 (vi) e (vii).

Quando a categoria $\mathcal{C}$ é **Sets**, obtem-se a definição anterior de feixes. Quando a categoria $\mathcal{C}$ é **Grp**, $\mathbf{Alg}_{\mathbb{K}}$ ou **Rng**, o feixe é dito *feixe de grupos*, *feixe de $\mathbb{K}$-álgebras* ou *feixe de anéis*, respectivamente.

Definição 3.1.57. Seja $(X, \mathcal{F}, \rho)$ um espaço topológico munido de feixe. Defina o *stalk* do feixe $\mathcal{F}$ em um ponto $x \in X$, como o limite direto da família $\{\mathcal{F}(U) \mid x \in U, U \subseteq X : \text{aberto}\}$, ou seja, $\mathcal{F}_x = \varinjlim_{U : x \in U} \mathcal{F}(U)$.

A ideia do stalk é a mesma ideia dos germes de funções da geometria diferencial. Ou seja, stalk é o conjunto de funções que são localmente regulares em torno de um ponto dado. Explicitamente, considere uma variedade afim X, dois abertos $U, V \subseteq X$ contendo um ponto $x \in X$, uma função f, regular em U e uma função g, regular em V. Então f é equivalente a g, quando existe um aberto $W \subseteq U \cap V$, contendo x, onde $f|_W = g|_W$, ou seja, quando as duas funções são localmente iguais.

Exemplo 3.1.58.

(i) Considere o espaço topológico $X = \mathbb{A}^n$. Para cada aberto $U \subseteq \mathbb{A}^n$, $\mathcal{O}_{\mathbb{A}^n}$ associa o anel de funções regulares em U. A restrição de funções regulares a subconjuntos faz o papel de ρ e as condições de feixe são satisfeitas. $\mathcal{O}_{\mathbb{A}^n}$ é chamado de *feixe estrutural em $\mathbb{A}^n$*. De uma forma geral, para toda variedade afim $X \subseteq \mathbb{A}^n$, $\mathcal{O}_X$ é um feixe em X. O stalk do feixe estrutural em cada ponto $p \in X$ é o anel local de funções regulares $\mathcal{O}_{X,p}$.

(ii) Considere o espaço topológico $X = \mathbb{P}^n$. A cada aberto $U \subseteq \mathbb{P}^n$, $\mathcal{O}_{\mathbb{P}^n}$ associa o anel de funções regulares em U. A restrição de funções regulares a subconjuntos faz o papel de ρ e as condições de feixe são satisfeitas. $\mathcal{O}_{\mathbb{P}^n}$ é chamado de *feixe estrutural em $\mathbb{P}^n$*. De uma forma geral, para toda variedade projetiva $Y \subseteq \mathbb{P}^n$, $\mathcal{O}_Y$ é um feixe em Y. O stalk do feixe estrutural em cada ponto $p \in Y$ é o anel local de funções regulares $\mathcal{O}_{Y,p}$.

Definição 3.1.59. Sejam $(X, \mathcal{F}, \rho)$ e $(X, \mathcal{F}', \rho')$ espaços topológicos munidos de feixes $\mathcal{F}, \mathcal{F}' : Top(X) \to \mathcal{C}$. Um *morfismo de feixes* é uma transformação natural $\varphi : \mathcal{F} \to \mathcal{F}'$, ou seja:

(i) Para todo aberto $U \subseteq X$, $\varphi(U) : \mathcal{F}(U) \to \mathcal{F}'(U)$ é um morfismo na categoria $\mathcal{C}$.

(ii) Dados $U \subseteq V$ dois abertos de X, o seguinte diagrama é comutativo:

$$\begin{tikzcd}
\mathcal{F}(V) \arrow[r, "\rho^V_U"] \arrow[d, "\varphi(V)"] & \mathcal{F}(U) \arrow[d, "\varphi(U)"] \\
\mathcal{F}'(V) \arrow[r, "{\rho'}^V_U"'] & \mathcal{F}'(U)
\end{tikzcd}$$

Um *isomorfismo de feixes* é um morfismo de feixes com inversa à esquerda e à direita.

Proposição 3.1.60. Sejam $\mathcal{F}$ e $\mathcal{F}'$ dois feixes sobre um espaço topológico X. Um morfismo de feixes $\varphi : \mathcal{F} \to \mathcal{F}'$ é um isomorfismo se, e somente se, para cada $p \in X$, os morfismos $\varphi_p : \mathcal{F}_p \to \mathcal{F}'_p$ induzidos nos stalks forem isomorfismos.

Dem: [Har], p.63. □

A partir de agora, considere apenas feixes de anéis.

Definição 3.1.61. Seja $(X, \mathcal{F}, \rho)$ um espaço topológico munido de feixe. Um *subfeixe* de $\mathcal{F}$ é um espaço topológico munido de feixe $(X, \mathcal{F}', \rho)$, tal que para cada aberto $U \subseteq X$, $\mathcal{F}'(U)$ é subanel de $\mathcal{F}(U)$.

Definição 3.1.62. Seja $(X, \mathcal{F}, \rho)$ um espaço topológico noetheriano munido de feixe. O espaço é chamado de *pré-variedade* quando existir uma cobertura finita por abertos $X = \bigcup_{i=1}^{k} U_i$ tal que cada um dos abertos com a topologia induzida e o feixe induzido $(U_i, \mathcal{F}_{U_i})$, onde $\mathcal{F}_{U_i}(V) = \mathcal{F}(V)$ para todo aberto $V \subseteq U_i$, é isomorfo a uma variedade afim munida do feixe de funções regulares. Ou seja, para cada $i = 1, \ldots, k$, existem uma variedade afim $V_i \subseteq \mathbb{A}^{n_i}$ e um homeomorfismo $\varphi_i : U_i \to V_i$, tal que o comorfismo $\varphi_i^* : \mathcal{O}_{V_i} \to \mathcal{F}_{U_i}$ é um isomorfismo de feixes.

Intuitivamente, uma pré-variedade é uma colagem de variedades afins.

Exemplo 3.1.63.

(i) Toda variedade afim munida do feixe de funções regulares é uma pré-variedade.

(ii) Toda variedade projetiva munida do feixe de funções regulares é uma pré-variedade. A cobertura aberta é feita pelos abertos afins munidos dos respectivos feixes de funções regulares.

Por analogia com esse segundo exemplo, define-se:

Definição 3.1.64. Seja X uma pré-variedade munida de um feixe $\mathcal{F}$. Um aberto $U \subseteq X$ munido do feixe $\mathcal{F}_U$ será dito *aberto afim de* X quando for isomorfo a uma variedade afim munida do feixe de funções regulares.

Definição 3.1.65. Sejam $(X, \mathcal{F}_X)$ e $(Y, \mathcal{F}_Y)$ duas pré-variedades munidas de feixes. Uma função $\varphi : X \to Y$ é um *morfismo de pré-variedades*, quando:

(i) φ é contínua;

(ii) Para todo aberto $V \subseteq Y$, $\varphi^*(g) = (g \circ \varphi) \in \mathcal{F}_X(\varphi^{-1}(V))$, $\forall\, g \in \mathcal{F}_Y(V)$.

Observe que a primeira condição é uma condição sobre a estrutura topológica da pré-variedade. Ela diz que esta estrutura é preservada, ou seja, para todo aberto $V \subseteq Y$ sua imagem inversa $\varphi^{-1}(V) \subseteq X$ também vai ser um aberto. Por isso faz sentido se perguntar sobre a estrutura das funções regulares em $\varphi^{-1}(V)$. A segunda condição diz que essa estrutura também é preservada.

Usando o fato de que pré-variedades são colagens de variedades afins, o seguinte teorema afirma que uma função entre pré-variedades é um morfismo se for um morfismo em cada aberto afim.

Teorema 3.1.66. Sejam X e Y duas pré-variedades com coberturas por abertos afins $X = \bigcup_i U_i$ e $Y = \bigcup_j V_j$. Seja $\varphi : X \to Y$ uma função entre as pré-variedades. Considere, para cada V_j, $\varphi^{-1}(V_j) \subset X$, decomponha $\varphi^{-1}(V_j) = \bigcup_i(\varphi^{-1}(V_j) \cap U_i)$, defina $U_{ij} = \varphi^{-1}(V_j) \cap U_i$ e defina $\varphi_{ij} = \varphi|_{U_{ij}}$. φ é um morfismo de pré-variedades se, e somente se, φ_{ij} são morfismos para todos os pares (i, j).

Dem: Considere um aberto $V \subseteq Y$. Como V é aberto em Y e φ_{ij} é morfismo, $\varphi_{ij}^{-1}(V \cap V_j)$ é aberto em U_{ij} e portanto é aberto em X. Como se pode escrever

$$\varphi^{-1}(V) = \bigcup_j \varphi^{-1}(V \cap V_j) = \bigcup_j \left(\bigcup_i \left(U_{ij} \cap \varphi^{-1}(V \cap V_j)\right) \right) = \bigcup_i \left(\bigcup_j \left(\varphi_{ij}^{-1}(V \cap V_j) \right) \right),$$

$\varphi^{-1}(V)$ é aberto e portanto φ é contínua. Agora basta provar que, para todo $f \in \mathcal{O}_Y(V)$, $f \circ \varphi \in \mathcal{O}_X(\varphi^{-1}(V))$. Como $\mathcal{O}_X$ é um feixe e $(f \circ \varphi)|_{\varphi^{-1}(V) \cap U_{ij}} = f|_{V \cap V_j} \circ \varphi_{ij}$, segue que $f \circ \varphi \in \mathcal{O}_X(\varphi^{-1}(V))$. $\square$

Exemplo 3.1.67.

(i) Sejam $(X, \mathcal{O}_X)$ e $(Y, \mathcal{O}_Y)$ duas variedades afins munidas dos respectivos feixes de funções regulares. Então $(\varphi, \varphi^*) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$, onde φ é um morfismo de variedades afins e φ^* é o comorfismo correspondente, é um morfismo de pré-variedades.

(ii) Sejam $(X, \mathcal{O}_X)$ e $(Y, \mathcal{O}_Y)$ duas variedades projetivas munidas dos respectivos feixes de funções regulares. Usando o teorema acima, $(\varphi, \varphi^*) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$, onde φ é um morfismo de variedades projetivas e φ^* é o comorfismo correspondente, é um morfismo de pré-variedades.

Definição 3.1.68. Uma *variedade* é uma pré-variedade X tal que a diagonal $\{(x, x) \in X \times X \mid x \in X\}$ é um subconjunto fechado de $X \times X$ com a topologia produto.

Exemplo 3.1.69.

(i) Toda variedade afim é uma variedade.

(ii) Toda variedade projetiva é uma variedade.

(iii) Produtos de variedades são variedades.

Definição 3.1.70. Seja X uma variedade algébrica. Um subconjunto $C \subseteq X$ é chamado de *construtível*, quando C for uma união finita de intersecções entre conjuntos abertos e fechados de X.

Proposição 3.1.71. Seja $\varphi : X \to Y$ um morfismo de variedades. Se $C \subseteq X$ é construtível então $\varphi(C) \subseteq Y$ também é construtível.

3.1.6 Esquemas

Nesta seção uma outra noção de variedade será apresentada. A ideia principal é a de abstrair do conjunto de pontos e se fixar mais no anel de funções regulares definidos nas seções anteriores.

Considere novamente $\mathbb{K}$ como um corpo algebricamente fechado.

Definição 3.1.72. Seja R um anel. Defina $Spec(R)$ como o conjunto de ideais primos de R. Para cada ideal $I \subseteq R$ defina a *variedade associada a* I como $V(I) = \{P \in Spec(R) \mid P \supseteq I\}$. Para cada $a \in R$ defina um *aberto principal* como $D(a) = (V(\langle a \rangle))^c$.

Proposição 3.1.73. Sejam R um anel e $\{P_i \mid i \in I\}$ uma família de ideais de R.

(i) $Spec(R) = V(0)$.

(ii) $\emptyset = V(R)$.

(iii) $\bigcap_{i\in I} V(P_i) = V\left(\sum_{i\in I} P_i\right)$.

(iv) $V(P_i) \cup V(P_j) = V(P_iP_j)$, $\forall\, i, j \in I$.

Dem:

(i) Por definição $V(0) = \{P \in Spec(R) \mid 0 \subseteq P\}$. Como todo ideal primo de R contem $\{0\}$, $V(0) = Spec(R)$.

(ii) Por definição $V(R) = \{P \in Spec(R) \mid R \subseteq P\}$. Como nenhum ideal primo de R pode conter R, $V(R) = \emptyset$.

(iii) Por definição $V\left(\sum_{i\in I} P_i\right)$ é o conjunto de ideais primos de R que contêm $\sum_{i\in I} P_i$. Portanto $V\left(\sum_{i\in I} P_i\right)$ é o conjunto de ideais primos de R que contêm todos os ideais primos P_i. Por outro lado, $\bigcap_{i\in I} V(P_i)$ é o conjunto de ideais primos de R que contêm os ideais P_i para todo i. Portanto $\bigcap_{i\in I} V(P_i)$ também é o conjunto de ideais primos de R que contêm todos os ideais primos P_i.

(iv) Por definição $V(P_i) \cup V(P_j)$ é o conjunto de ideais primos de R que contêm P_i ou P_j. Por outro lado, $V(P_iP_j)$ é o conjunto de ideais primos de R que contêm P_iP_j. Mas $P_iP_j \subseteq P$ implica que P contém P_i ou P_j. Portanto $V(P_iP_j)$ também é o conjunto de ideais primos de R que contêm P_i ou P_j.

$\square$

A proposição anterior sugere que os conjuntos $Spec(R)$ admitem uma topologia.

Definição 3.1.74. Seja R um anel. Mune-se o conjunto $Spec(R)$ com a *topologia de Zariski* definindo os fechados de $Spec(R)$ como as variedades, ou seja, $X \subseteq Spec(R)$ é fechado quando existe um ideal $I \subseteq R$ tal que $V(I) = X$.

Com isso, a todo anel R está associado um espaço topológico, a saber, $Spec(R)$ munido da topologia de Zariski. As variedades são os fechados de $Spec(R)$ e os conjuntos $D(a)$, $a \in R$, são abertos em $Spec(R)$.

Exemplo 3.1.75.

(*i*) Considere o anel $\mathbb{K}[x_1, \ldots, x_n]$. Os ideais primos de $\mathbb{K}[x_1, \ldots, x_n]$ determinam variedades irredutíveis em $\mathbb{A}^n$. Portanto os pontos do espaço $Spec(\mathbb{K}[x_1, \ldots, x_n])$ podem ser identificados com as variedades irredutíveis de $\mathbb{A}^n$. As subvariedades de $Spec(\mathbb{K}[x_1, \ldots, x_n])$ são definidas como os conjuntos de ideais primos de $\mathbb{K}[x_1, \ldots, x_n]$ contendo um certo ideal primo P. Ou seja, a variedade $V(P) \subseteq Spec(\mathbb{K}[x_1, \ldots, x_n])$ pode ser identificada com o conjunto das subvariedades irredutíveis da variedade irredutível afim $V(P) \subseteq \mathbb{A}^n$. Portanto $V(P) \subseteq Spec(\mathbb{K}[x_1, \ldots, x_n])$ e $V(P) \subseteq \mathbb{A}^n$ têm significados diferentes. Em particular, $Spec(\mathbb{K}[x_1, \ldots, x_n])$ e $\mathbb{A}^n$ não podem ser identificados.

Considere um ponto P em $Spec(\mathbb{K}[x_1, \ldots, x_n])$. Sabe-se que $V(P)$ é fechado em $Spec(\mathbb{K}[x_1, \ldots, x_n])$. Ainda mais, esse é o menor fechado contendo P. Portanto, para todo ponto $P \in Spec(\mathbb{K}[x_1, \ldots, x_n])$, $V(P)$ é o fecho do conjunto $\{P\}$. Um ponto $P \in Spec(\mathbb{K}[x_1, \ldots, x_n])$ é fechado se, e somente se, P for um ideal maximal em $\mathbb{K}[x_1, \ldots, x_n]$. O espaço afim $\mathbb{A}^n$ pode, agora, ser identificado com o conjunto de pontos fechados de $Spec(\mathbb{K}[x_1, \ldots, x_n])$. Os outros pontos, ou seja, as outras variedades irredutíveis afins são chamadas de *pontos genéricos de* $Spec(\mathbb{K}[x_1, \ldots, x_n])$.

(*ii*) Considere $X \subseteq \mathbb{A}^n$ uma variedade afim. De forma análoga ao espaço afim, X pode ser visto como o conjunto de pontos fechados de $Spec(\mathbb{K}[X])$. As outras subvariedades irredutíveis de X são os pontos genéricos de $Spec(\mathbb{K}[X])$.

Definição 3.1.76. Seja R um anel. Define-se o *feixe estrutural* ou *feixe de funções regulares* no espaço topológico $Spec(R)$ como o feixe de anéis $\mathcal{O}$ que associa a cada aberto $U \subseteq Spec(R)$, o anel de funções $f : U \to \coprod_{P \in U} R_P$ tais que:

(*i*) Para cada $P \in U$, $f(P) \in R_P$;

(*ii*) Para cada $P \in U$, existem um aberto $A \subseteq U$, $P \in A$, e elementos $r, s \in R$, $s \notin \left(\bigcup_{\wp \in A} \wp\right)$, para os quais $f(a) = (r, s) \in R_P$ para todo $a \in A$. Ou seja, localmente f é um quociente de elementos de R.

Definição 3.1.77. Seja R um anel. Define-se o *Spectrum de* R como o espaço topológico $Spec(R)$ munido do feixe estrutural $\mathcal{O}$.

Exemplo 3.1.78.

(*i*) Considere o espaço topológico $X = Spec(\mathbb{K}[x_1, \ldots, x_n])$. Como já foi descrito, $Spec(\mathbb{K}[x_1, \ldots, x_n])$ é identificado com o conjunto de subvariedades irredutíveis de $\mathbb{A}^n$. É natural tentar identificar o feixe estrutural $\mathcal{O}_X$ com o feixe de funções regulares de $\mathbb{A}^n$. De fato, o feixe estrutural $\mathcal{O}_X$ associa a cada aberto $U \subseteq Spec(\mathbb{K}[x_1, \ldots, x_n])$ o conjunto de funções $f : U \to \coprod_{P \in U} \mathbb{K}[x_1, \ldots, x_n]_P$, tais que, para cada $\mathfrak{p} \in U$, $f(\mathfrak{p}) = g/h \in \mathbb{K}[x_1, \ldots, x_n]_{\mathfrak{p}}$, ou seja, $h \notin I(\{\mathfrak{p}\})$, e existe um aberto $V \subseteq U$, tal que $f(\mathfrak{q}) = g'/h'$ para todo $\mathfrak{q} \in V$.

Isso significa que $\mathcal{O}_X(U)$ é o conjunto de funções regulares em U como definido na seção 3.1.2.

(*ii*) Considere $X \subseteq \mathbb{A}^n$ uma variedade afim e $Y = Spec(\mathbb{K}[X])$. De maneira análoga ao exemplo anterior, o feixe estrutural em Y associa a cada aberto $U \subseteq Y$ o conjunto de funções de U, visto como aberto de $Spec(\mathbb{K}[X])$, para as funções regulares em U visto como aberto da variedade afim X.

Proposição 3.1.79. Sejam R um anel e $(Spec(R), \mathcal{O})$ seu Spectrum.

(*i*) Para todo $P \in Spec(R)$, o stalk do feixe estrutural em P é isomorfo ao anel local R_P.

(*ii*) Para todo elemento $a \in R$, o anel $\mathcal{O}(D(a))$ é isomorfo ao anel local $(R \setminus \langle a \rangle)^{-1}R$.

(*iii*) $\mathcal{O}(Spec(R))$ é isomorfo ao anel R.

Dem:

(*i*) Considere o morfismo $\varphi : \mathcal{O}_P \to R_P$ que a cada seção local $f \in \mathcal{O}(U)$, com $P \in U$, associa o valor da seção f no ponto P, ou seja, $\varphi(f) = f(P)$. Esta função é sobrejetiva, porque todo elemento de R_P pode ser escrito como a/b, onde $a, b \in R$ e $b \notin P$. Nesse caso, $D(b)$ é um aberto contendo P e a/b define uma seção em $\mathcal{O}(D(b))$ cujo valor em P é a/b. Para mostrar que φ é injetora, considere um aberto U contendo P e duas seções locais $f, g \in \mathcal{O}(U)$ tais que $\varphi(f) = \varphi(g)$, ou seja, $f(P) = g(P)$. Considere U pequeno o suficiente de modo que seja possível escrever $f = a/b$ e $g = c/d$, onde $a, b, c, d \in R$ e $b, d \notin P$. Como $\varphi(a/b) = \varphi(c/d) \in R_P$, existe um elemento $x \in R \setminus P$ tal que $x(ad - bc) = 0 \in R$. Então $a/b = c/d$ em qualquer anel local R_Q onde $b, d, x \notin Q$. O conjunto de tais pontos é $D(b) \cap D(d) \cap D(x)$ que por sua vez é um aberto contendo P. Isso significa que $f = g$ numa vizinhança de P e portanto $f = g$ em $\mathcal{O}_P$. Portanto φ é injetora e consequentemente um isomorfismo.

(*ii*) Para mostrar que $\mathcal{O}(D(a))$ é isomorfo a $R_{\langle a \rangle}$, defina o morfismo $\psi : R_{\langle a \rangle} \to \mathcal{O}(D(a))$ que a cada elemento $x/a^n \in R_{\langle a \rangle}$ associa a seção $f \in \mathcal{O}(D(a))$ tal que $f(P) = x/a^n$. Para mostrar que ψ é injetivo, considere $x/a^n, y/a^m \in R_{\langle a \rangle}$ tais que $\psi(x/a^n) = \psi(y/a^m)$. Isso significa que para todo $P \in D(a)$, x/a^n e y/a^m tem a mesma imagem em R_P e portanto existe $z \in R \setminus P$ tal que $z(xf^m - yf^n) = 0$. Considere $\mathfrak{a}$ como o ideal de R gerado pelos elementos que anulam $(xf^m - yf^n)$. Como $z \in \mathfrak{a}$ e $z \notin P$, $\mathfrak{a} \subsetneq P$. Como isso vale para todo $P \in D(a)$, $V(\mathfrak{a}) \cap D(a) = \emptyset$. Logo $a \in \sqrt{\mathfrak{a}}$, ou seja, existe $l \in \mathbb{N}$ tal que $a^l \in \mathfrak{a}$ e portanto $a^l(xa^m - ya^n) = 0$. Isso mostra que $x/a^n = y/a^m$, o que implica que ψ é injetivo. Para mostrar a sobrejetividade, vide [Har], p.71,72.

(*iii*) Usando o item anterior quando $a = 1$ e $D(1) = Spec(R)$, esse caso particular é demonstrado.

□

Definição 3.1.80. Sejam X e Y dois espaços topológicos e $f : X \to Y$ uma função contínua. Para um feixe $\mathcal{F}$ em X, define-se a *imagem direta* de $\mathcal{F}$, $f_*\mathcal{F}$, como o feixe em Y tal que para cada aberto $V \subseteq Y$, $f_*\mathcal{F}(V) = \mathcal{F}(f^{-1}(V))$.

Definição 3.1.81. Um *espaço anelado* é um espaço topológico munido de um feixe de anéis $(X, \mathcal{O}_X)$. Um morfismo entre dois espaços anelados $(X, \mathcal{O}_X)$ e $(Y, \mathcal{O}_Y)$ é um par (φ, φ^*), tal que $\varphi : X \to Y$ é uma função contínua e $\varphi^* : \mathcal{O}_Y \to \varphi_*\mathcal{O}_X$ é um morfismo de feixes de anéis.

Um *espaço localmente anelado* é um espaço anelado $(X, \mathcal{O}_X)$, tal que para todo ponto $P \in X$, o stalk $\mathcal{O}_{X,P}$ é um anel local. Um morfismo de espaços localmente anelados, $(\varphi, \varphi^*) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$, é um morfismo de espaços anelados tal que, para cada ponto $P \in X$, o morfismo induzido $\varphi_P^* : \mathcal{O}_{Y,\varphi(P)} \to \mathcal{O}_{X,P}$ é um morfismo local de anéis locais, ou seja, o morfismo induzido satisfaz $(\varphi_P^*)^{-1}(\mathfrak{m}_P) = \mathfrak{m}_{\varphi(P)}$.

Exemplo 3.1.82.

(i) Pela proposição 3.1.79, todo Spectrum de um anel é um espaço localmente anelado.

(ii) Considere $X \subseteq \mathbb{A}^n$ uma variedade afim. Como já foi descrito nos exemplos anteriores $(Spec(\mathbb{K}[X]), \mathcal{O}_{Spec(\mathbb{K}[X])})$ é um espaço localmente anelado.

(iii) Considere duas variedades afins $X \subseteq \mathbb{A}^n$ e $Y \subseteq \mathbb{A}^m$. Como já foi descrito a todo morfismo entre variedades afins $\varphi : X \to Y$ está associado um único morfismo entre as álgebras afins $\varphi^* : \mathbb{K}[Y] \to \mathbb{K}[X]$, chamado de comorfismo. Considere, agora, os espaços localmente anelados $(Spec(\mathbb{K}[X]), \mathcal{O}_{Spec(\mathbb{K}[X])})$ e $(Spec(\mathbb{K}[Y]), \mathcal{O}_{Spec(\mathbb{K}[Y])})$. O morfismo φ e o comorfismo φ^* induzem um morfismo entre os espaços localmente anelados $(\varphi, \varphi^*) : (Spec(\mathbb{K}[X]), \mathcal{O}_{Spec(\mathbb{K}[X])}) \to (Spec(\mathbb{K}[Y]), \mathcal{O}_{Spec(\mathbb{K}[Y])})$.

Definição 3.1.83. Um *esquema afim* é um espaço localmente anelado isomorfo (como espaço localmente anelado) ao spectrum de um anel. Um *esquema* é um espaço localmente anelado $(X, \mathcal{O}_X)$ que é localmente um esquema afim, ou seja, para todo ponto $P \in X$ existe um aberto $U \subseteq X$, $P \in U$, tal que o espaço localmente anelado $(U, \mathcal{O}_X|_U)$, onde $\mathcal{O}|_U(V) = \mathcal{O}_X(V)$ para todo aberto $V \subseteq U$, é um esquema afim. Um *morfismo de esquemas* é um morfismo de espaços localmente anelados.

Definição 3.1.84. Um anel R é dito *graduado* quando existir uma decomposição $R = \oplus_{d \in \mathbb{N}} R_d$, tal que, para cada $d \in \mathbb{N}$, R_d é um grupo abeliano satisfazendo $R_a R_b \subseteq R_{a+b}$, $\forall\, a, b \in \mathbb{N}$. Um elemento de $r \in R$ é dito *homogêneo de grau d* quando $r \in R_d$. Um ideal $I \subseteq R$ é dito *homogêneo* quando puder ser gerado por elementos homogêneos de R.

Seja R um anel graduado. Defina o *ideal trivial de R* como $R_+ = \oplus_{d \in \mathbb{N}^\bullet} R_d$. Defina também $Proj(R)$ como o conjunto dos ideais primos homogêneos de R que não contêm R_+.

Para cada ideal homogêneo $I \subseteq R$ defina a *variedade associada a I* como $V(I) = \{P \in Proj(R) \mid P \supseteq I\}$. Para cada elemento homogêneo $f \in R_+$ defina o *aberto principal associado a f* como $D_+(f) = \{P \in Proj(R) \mid f \notin P\}$.

Proposição 3.1.85. Sejam R um anel graduado e $\{P_i \mid i \in I\}$ uma família de ideais homogêneos de R.

(i) $Proj(R) = V(0)$.

(ii) $\emptyset = V(R)$.

(iii) $\bigcap_{i \in I} V(P_i) = V\left(\sum_{i \in I} P_i\right)$.

(iv) $V(P_i) \cup V(P_j) = V(P_i P_j)$, $\forall\, i, j \in I$.

A proposição anterior sugere que os conjuntos $Proj(R)$ admitem uma topologia.

Definição 3.1.86. Seja R um anel graduado. Mune-se o conjunto $Proj(R)$ com uma topologia definindo os fechados de $Proj(R)$ como as variedades, ou seja, $X \subseteq Proj(R)$ é fechado, quando existe um ideal homogêneo $I \subseteq R$, tal que $V(I) = X$.

Com isso, a todo anel graduado R está associado um espaço topológico, a saber, $Proj(R)$ munido da topologia descrita acima. As variedades são os fechados de $Proj(R)$ e os conjuntos $D_+(a)$, a homogêneo em R, são abertos em $Proj(R)$.

Exemplo 3.1.87.

(i) Considere o anel $\mathbb{K}[x_0, \ldots, x_n]_h$. Os ideais primos homogêneos de $\mathbb{K}[x_0, \ldots, x_n]_h$ determinam variedades irredutíveis em $\mathbb{P}^n$. Portanto os pontos de $Proj(\mathbb{K}[x_0, \ldots, x_n]_h)$ podem ser identificados com as variedades irredutíveis de $\mathbb{P}^n$. As variedades irredutíveis de $Proj(\mathbb{K}[x_0, \ldots, x_n]_h)$ são definidas como os conjuntos de ideais primos homogêneos de $\mathbb{K}[x_0, \ldots, x_n]_h$ contendo um certo ideal homogêneo primo P. Ou seja, a variedade $V(P) \subseteq Proj(\mathbb{K}[x_0, \ldots, x_n]_h)$ pode ser identificada com o conjunto de todas as subvariedades irredutíveis da variedade irredutível projetiva $V(P) \subseteq \mathbb{P}^n$. Portanto $V(P) \subseteq Proj(\mathbb{K}[x_0, \ldots, x_n]_h)$ e $V(P) \subseteq \mathbb{P}^n$ têm significados diferentes. Em particular, $Proj(\mathbb{K}[x_0, \ldots, x_n]_h)$ e $\mathbb{P}^n$ não podem ser identificados.

Definição 3.1.88. Seja R um anel graduado. Para cada $P \in Proj(R)$ considere T o sistema multiplicativo formado pelos elementos homogêneos de R que não pertencem a P. Defina $R_{(P)}$ como o conjunto de elementos de grau zero em $T^{-1}R$.

Define-se o *feixe estrutural* ou *feixe de funções regulares* no espaço topológico $Proj(R)$ como o feixe de anéis $\mathcal{O}$ que associa a cada aberto $U \subseteq Proj(R)$, o anel graduado de funções $f : U \to \coprod_{P \in U} R_{(P)}$ tais que:

(i) Para cada $P \in U$, $f(P) \in R_{(P)}$;

(ii) Para cada $P \in U$, existem um aberto $A \subseteq U$, $P \in A$, e elementos $r, s \in R$, $s \notin \left(\bigcup_{\wp \in A} \wp\right)$, para os quais $f(a) = (r, s) \in R_{(P)}$ para todo $a \in A$. Ou seja, localmente f é um quociente de elementos de R.

Exemplo 3.1.89.

(i) Considere o espaço topológico $X = Proj(\mathbb{K}[x_0, \ldots, x_n]_h)$. Como já foi descrito, $Proj(\mathbb{K}[x_1, \ldots, x_n]_h)$ é identificado com o conjunto de subvariedades irredutíveis de $\mathbb{P}^n$. É natural tentar identificar o feixe estrutural $\mathcal{O}_X$ com o feixe de funções regulares de $\mathbb{P}^n$. De fato, o feixe estrutural $\mathcal{O}_X$ associa a cada aberto $U \subseteq Proj(\mathbb{K}[x_0, \ldots, x_n]_h)$ o conjunto de funções $f : U \to \coprod_{P \in U} \mathbb{K}[x_0, \ldots, x_n]_{(P)}$, tais que, para cada $\mathfrak{p} \in U$, $f(\mathfrak{p}) = g/h \in \mathbb{K}[x_0, \ldots, x_n]_{(\mathfrak{p})}$, ou seja, $h \notin I(\{\mathfrak{p}\})$, e existe um aberto $V \subseteq U$, tal que $f(\mathfrak{q}) = g'/h'$ para todo $\mathfrak{q} \in V$.

Isso significa que $\mathcal{O}_X(U)$ é o conjunto de funções regulares em U como definido na seção 3.1.4.

(ii) Considere $X \subseteq \mathbb{P}^n$ uma variedade projetiva e $Y = Proj(\mathbb{K}[X])$. De maneira análoga ao exemplo anterior, o feixe estrutural em Y associa a cada aberto $U \subseteq Y$ o conjunto de funções de U, visto como aberto de $Proj(\mathbb{K}[X])$, para as funções regulares em U visto como aberto da variedade projetiva X.

Proposição 3.1.90. Sejam R um anel graduado e $(Proj(R), \mathcal{O})$ como acima.

(i) Para todo $P \in Proj(R)$, o stalk do feixe estrutural em P é isomorfo ao anel local $R_{(P)}$.

(ii) Para todo elemento homogêneo $a \in R_+$, existe um isomorfismo de anéis localmente anelados entre $(D_+(a), \mathcal{O}_{D_+(a)})$ e $Spec(R_{(\langle a \rangle)})$.

(iii) $Proj(R)$ é um esquema.

3.1.7 Funtores

Nesta seção vamos introduzir a noção de R-funtor que, na linguagem funtorial, é um análogo às variedades como definidas nas seções anteriores. Se por um lado a intuição de variedade algébrica (como conjunto de zeros de polinômios) fica prejudicada nesta linguagem, por outro lado, a estensão da noção de variedade e solução dos respectivos problemas para o caso de dimensão infinita parecem viáveis. A referência para esta seção é [Jan].

A ideia de R-funtor vem do Nullstellensatz. Esse teorema diz que dada X uma variedade afim sobre $\mathbb{K}$, então $Hom_{Alg_{\mathbb{K}}}(\mathbb{K}[X], \mathbb{K}) = X$ na categoria de conjuntos. Ou seja, os pontos de uma variedade afim sobre $\mathbb{K}$ são determinados pelos morfismos da sua álgebra afim sobre $\mathbb{K}$.

Definição 3.1.91. Seja R um anel. Um funtor X da categoria de R-álgebras para a categoria de conjuntos é chamado de *R-funtor*. Um *subfuntor* de X é um R-funtor Y tal que, para cada $A \in \mathbf{Alg}_R$, $Y(A) \subseteq X(A)$ e, para cada morfismo entre R-álgebras, $\varphi \in Hom_{Alg_R}(A, A')$, $Y(\varphi) = X(\varphi)|_{Y(A)}$. Um *morfismo* entre dois R-funtores é uma transformação natural entre esses funtores.

Agora que construímos a categoria de R-funtores, ou seja, a categoria cujos objetos são R-funtores e os morfismos são transformações naturais entre eles, é natural se perguntar se as construções feitas para variedades afins e para esquemas têm análogos nesta categoria.

Definição 3.1.92. Seja R um anel.

(i) Seja $\{Y_i \mid i \in I\}$ uma família de subfuntores de um R-funtor X. Definimos a *interseção* $Y = \bigcap_{i \in I} Y_i$ como um R-funtor que associa a cada $A \in \mathbf{Alg}_R$, $Y(A) = \bigcap_{i \in I}(Y_i(A))$ e a cada morfismo entre R-álgebras, $\varphi \in Hom_{Alg_R}(A, A')$, $Y(\varphi) = X(\varphi)|_{Y(A)}$.

(ii) Sejam X, Y dois R-funtores e $f \in Hom(X, Y)$ uma transformação natural de X para Y. Para cada subfuntor $Y' \subseteq Y$, defina a *imagem inversa* de Y' por f como o subfuntor $f^{-1}(Y') \subseteq X$ tal que, para cada $A \in \mathbf{Alg}_R$, $f^{-1}Y'(A) = f_A^{-1}(Y'(A))$.

(iii) Sejam X e Y dois R-funtores. Defina o *produto* $X \times Y$ como o R-funtor que, para cada $A \in \mathbf{Alg}_R$, associa $(X \times Y)(A) = X(A) \times Y(A)$.

Na teoria de variedades definimos as variedades afins e na teoria de esquemas definimos os esquemas afins. Um análogo funtorial é o seguinte.

Definição 3.1.93. Seja R um anel. Um *R-funtor afim de dimensão n* é um R-funtor, denotado por $\mathbb{A}^n$, que associa, a cada $A \in \mathbf{Alg}_R$, $\mathbb{A}^n(A) = A^n$ e, a cada morfismo $\varphi \in Hom_{Alg_R}(A, A')$, $\mathbb{A}^n(\varphi) = \varphi^n : (a_1, \ldots, a_n) \mapsto (\varphi(a_1), \ldots, \varphi(a_n))$.

Exemplo 3.1.94. Considere o espaço afim n-dimensional sobre $\mathbb{K}$ e considere sua álgebra de funções regulares $\mathbb{K}[x_1, \ldots, x_n]$. A função $Hom_{Alg_{\mathbb{K}}}(\mathbb{K}[\mathbb{A}^n], \cdot)$ que, a cada $\mathbb{K}$-álgebra A, associa o conjunto $Hom_{Alg_{\mathbb{K}}}(\mathbb{K}[\mathbb{A}^n], A)$ é um $\mathbb{K}$-funtor afim.

De uma forma geral, seja $X \subseteq \mathbb{A}^n$ uma variedade afim. A função $Hom_{Alg_{\mathbb{K}}}(\mathbb{K}[X], \cdot)$ que a cada $\mathbb{K}$-álgebra A associa o conjunto $Hom_{Alg_{\mathbb{K}}}(\mathbb{K}[X], A)$ é um $\mathbb{K}$-funtor. Tal $\mathbb{K}$-funtor é subfuntor do funtor afim $Hom_{Alg_{\mathbb{K}}}(\mathbb{K}[\mathbb{A}^n], \cdot)$.

Pelo exemplo anterior, percebe-se que alguns importantes R-funtores são funtores representáveis.

Definição 3.1.95. Sejam R um anel e $\mathcal{A}_0$ uma R-álgebra. Defina o R-funtor $Sp_R\mathcal{A}_0$, chamado de *spectrum de* $\mathcal{A}_0$, da seguinte forma:

(*i*) $Sp_R\mathcal{A}_0(A) = Hom_{Alg_R}(\mathcal{A}_0, A)$ para todo $A \in \mathbf{Alg}_R$;

(*ii*) $Sp_R\mathcal{A}_0(\varphi) : Hom_{Alg_R}(\mathcal{A}_0, A) \to Hom_{Alg_R}(\mathcal{A}_0, A')$, $Sp_R\mathcal{A}_0(\varphi)(\alpha) = \varphi \circ \alpha$ para quaisquer $\varphi \in Hom_{Alg_R}(A, A')$ e $\alpha \in Hom_{Alg_R}(\mathcal{A}_0, A)$.

Quando não causar confusão, donotaremos o R-funtor afim $Sp_R\mathcal{A}$ por $Sp\mathcal{A}$.

Um R-funtor X é chamado de *funtor de esquema afim* ou R-*esquema afim* quando existe $\mathcal{A} \in Alg_R$, tal que X é isomorfo a $Sp_R\mathcal{A}$.

Observe que a partir de uma variedade afim X sobre $\mathbb{K}$, podemos obter um funtor de esquema afim, a saber, $Sp_{\mathbb{K}}\mathbb{K}[X]$.

Como existe uma equivalência de categorias entre as variedades afins e as álgebras finitamente geradas e reduzidas, gostaríamos de reconstruir uma álgebra a partir do funtor de esquema afim. Usando o Lema de Yoneda (1.5.9), obtem-se a seguinte proposição:

Proposição 3.1.96. Sejam R um anel e $\mathcal{A}$ uma R-álgebra. Para todo R-funtor X, existe uma bijeção entre $Hom(Sp_R\mathcal{A}, X)$ e $X(\mathcal{A})$.

Esta proposição permite definir intrinsecamente uma R-álgebra a partir do R-funtor, a saber, $Hom(X, \mathbb{A}^1)$. Esta álgebra coincide com o anel de funções regulares no caso das variedades afins (seção 3.1.1) e com a seção global no caso dos esquemas da seção 3.1.6. Por isso denota-se $Hom(X, \mathbb{A}^1)$ por $R[X]$.

Além disso, a proposição acima associa a cada Spectrum um morfismo de álgebras da seguinte forma:

Corolário 3.1.97. Sejam $\mathcal{A}$ e $\mathcal{A}'$ duas R-álgebras. Existe uma bijeção entre os conjuntos $Hom(Sp_R\mathcal{A}, Sp_R\mathcal{A}')$ e $Hom(\mathcal{A}', \mathcal{A})$.

Ou seja, a cada transformação natural entre R-funtores, corresponde um único morfismo entre R-álgebras. Esse morfismo coincide com o comorfismo no caso das variedades afins (seção 3.1.1) e dos esquemas da seção 3.1.6. Por isso, para cada transformação natural $f \in Hom(Sp_R\mathcal{A}, Sp_R\mathcal{A}')$, o correspondente morfismo de R-álgebras é denotado por $f^* \in Hom(\mathcal{A}', \mathcal{A})$ e chamado de *comorfismo*.

Usando as propriedades universais do produto de R-funtores e do produto tensorial de álgebras, obtemos a seguinte proposição:

Proposição 3.1.98. Sejam R um anel e X, Y R-funtores. Então $R[X \times Y] \simeq R[X] \otimes_R R[Y]$.

Definição 3.1.99. Seja R um anel. Um R-esquema afim X é chamado de *algébrico* quando existe $n \in \mathbb{N}^\bullet$, tal que $R[X] \simeq R[x_1, \ldots, x_n]/I$ para algum ideal $I \subseteq R[x_1, \ldots, x_n]$. O funtor de esquema afim X é chamado de *reduzido* quando $R[X]$ não contém elementos nilpotentes diferentes de 0.

Considere X uma $\mathbb{K}$-variedade afim. Usando a equivalência de categorias descrita na seção 3.1.2, existe uma única $\mathbb{K}$-álgebra finitamente gerada e reduzida associada a X, a saber, $\mathbb{K}[X]$. Considere agora o $\mathbb{K}$-funtor de esquema afim $\mathcal{X} = Sp\mathbb{K}[X]$. Usando a proposição 3.1.96, temos que $\mathbb{K}[\mathcal{X}] = \mathbb{K}[X]$. Portanto, $\mathcal{X}$ é um funtor de esquema afim algébrico e reduzido.

Por outro lado, considere um $\mathbb{K}$-funtor de esquema afim $\mathcal{X}$ algébrico e reduzido. Por definição, $\mathbb{K}[\mathcal{X}]$ é uma $\mathbb{K}$-álgebra finitamente gerada e reduzida. Usando a equivalência de categorias da seção 3.1.2, existe uma variedade afim X, tal que $\mathbb{K}[X] = \mathbb{K}[\mathcal{X}]$.

3.2 Dimensão

Uma classe de exemplos de variedades algébricas são as curvas algébricas planas. Intuitivamente, as curvas são objetos de dimensão 1, pois só necessitam de um parâmetro para serem descritas. Como estender esta mesma ideia para variedades em dimensões maiores? A intenção é tentar traduzir a ideia de "número de parâmetros necessários para descrever a variedade" de forma algébrica.

Durante esta seção, considere que $\mathbb{K}$ é um corpo algebricamente fechado.

Definição 3.2.1. Seja X uma variedade algébrica irredutível munida do feixe $\mathcal{O}_X$. O *corpo de funções racionais de* X é a classe de equivalência de todas as funções regulares em algum ponto de X, isto é, $\mathbb{K}(X) = \{f : X \to \mathbb{A}^1 |\ \exists\, U \subseteq X$ aberto não vazio, tal que $f \in \mathcal{O}_X(U)\}$, onde $f \simeq g$ quando existe um aberto $W \subseteq X$, tal que $f|_W = g|_W$.

O conjunto de funções racionais de uma variedade X tem de fato uma estrutura de corpo. Dadas duas funções racionais $f \in \mathcal{O}_X(U)$ e $g \in \mathcal{O}_X(V)$ definidas em abertos U, V da variedade X:

(i) $(f+g)(x) = f(x) + g(x),\ \forall\, x \in U \cap V$ e

(ii) $(fg)(x) = f(x)g(x),\ \forall\, x \in U \cap V$.

Como $f+g$ e fg são funções regulares em um aberto de X, a saber $U \cap V$, $f+g$ e fg são também racionais em X.

De uma forma análoga, para cada $f \in \mathcal{O}_X(U) \setminus \{0\}$ existe uma inversa $g \in \mathcal{O}_X(W)$, tal que: *(i)* W é o aberto de U onde f é não nula e *(ii)* $fg = 1$, em W.

Exemplo 3.2.2. Seja X uma variedade afim irredutível, ou seja, $X = V(I)$ onde I é um ideal primo $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Nesse caso, o corpo de funções racionais de X é dado pelo corpo de frações de $\mathbb{K}[X]$. Para provar isso, basta ver que para todo polinômio $f \in \mathbb{K}[X] \setminus \{0\}$, $1/f$ é regular em algum aberto de X. Considere a subvariedade fechada definida por $V(\langle f \rangle)$. Seu complementar é o aberto $D(f) \subseteq X$ onde f não se anula. Portanto $1/f$ é regular em $D(f)$.

Considere uma variedade algébrica sobre $\mathbb{K}$. Por construção, o corpo de funções racionais de X é um sobrecorpo do corpo $\mathbb{K}$ e, portanto, é natural a seguinte definição.

Definição 3.2.3. Se X for uma variedade irredutível, defina a *dimensão de* X como o grau de transcendência do seu corpo de funções racionais sobre $\mathbb{K}$. Se X não for uma variedade irredutível, decomponha X em componentes irredutíveis, $X = X_1 \cup \ldots \cup X_k$, e defina a *dimensão de* X como a maior dimensão entre as componentes irredutíveis de X, ou seja, $\dim(X) = max\{\dim(X_i) \mid i = 1, \ldots, k\}$.

As pré-variedades foram definidas como colagens de variedades afins de dimensão finita. Portanto toda variedade tem dimensão finita. Além disso, o corpo de funções racionais não muda se considerarmos um aberto afim, ou seja, dada uma variedade X, $\mathbb{K}(X) \simeq \mathbb{K}(U)$ para qualquer aberto afim $U \subseteq X$. Usando esse fato, não se perde generalidade ao tratar o caso de variedades afins.

Exemplo 3.2.4.

(i) O corpo de funções racionais do espaço afim $\mathbb{A}^n$ é isomorfo a $\mathbb{K}(x_1, \ldots, x_n)$. Portanto $\dim(\mathbb{A}^n) = n$.

(ii) O corpo de funções racionais do espaço projetivo $\mathbb{P}^n$ é isomorfo a $\mathbb{K}(x_1, \ldots, x_n)$. Portanto $\dim(\mathbb{P}^n) = n$.

(iii) Considere $X = V(\langle f \rangle)$ com $f(x, y) = y^2 - x \in \mathbb{C}[x, y]$. Nesse caso, X é uma parábola, que intuitivamente tem dimensão 1. Pela definição, $\mathbb{C}(X) \simeq \{\frac{g}{h} | g = \sum_{(i,j)} a_{ij} y^{2i+j}$ *e* $h = \sum_{(i,j)} b_{ij} y^{2i+j} \neq 0; a_{ij}, b_{ij} \in \mathbb{C}\}$. Portanto $\mathbb{C}(X) \simeq \mathbb{C}(y)$ e seu grau de transcendência é 1. Logo a dimensão de X é 1, como esperado.

(iv) A dimensão de $Gl_n(\mathbb{K})$ é n^2. O corpo de funções regulares de $Gl_n(\mathbb{K})$ é dado por $\mathbb{K}(x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn})$. Portanto seu grau de transcendência é n^2.

(v) A dimensão de $Sl_n(\mathbb{K})$ é $n^2 - 1$. De fato, o grau de transcendência do corpo de frações de $\mathbb{K}[Sl_n] \simeq \mathbb{K}[x_{11}, x_{12}, \ldots, x_{nn-1}, x_{nn}]/\langle \det -1 \rangle$ (conforme 3.1.20 (iv)) é $n^2 - 1$.

(vi) A dimensão de $T_n(\mathbb{K})$ é $\frac{n(n+1)}{2}$. De fato, o grau de transcendência do corpo de frações de $\mathbb{K}[T_n] \simeq \mathbb{K}[x_{ij} : 1 \leq i \leq j \leq n]$ (conforme 3.1.20 (v)) é $\frac{n(n+1)}{2}$.

(vii) A dimensão de $U_n(\mathbb{K})$ é $\frac{n(n-1)}{2}$. De fato, o grau de transcendência do corpo de frações de $\mathbb{K}[U_n] \simeq \mathbb{K}[x_{ij} : 1 \leq i < j \leq n]$ (conforme 3.1.20 (vi)) é $\frac{n(n-1)}{2}$.

($viii$) A dimensão de $D_n(\mathbb{K})$ é n. De fato, o corpo de frações de $\mathbb{K}[D_n] \simeq \mathbb{K}(x_{11}, \ldots, x_{nn})$ (conforme 3.1.20 (vi)). Portanto seu grau de transcendência é n.

Proposição 3.2.5. Sejam X e Y duas variedades algébricas irredutíveis. Então $\dim(X \times Y) = \dim(X) + \dim(Y)$.

Dem: Sem perda de generalidade assuma X e Y duas variedades irredutíveis e afins, $X \subseteq \mathbb{A}^p$ e $Y \subseteq \mathbb{A}^q$. Considere também $S_1, \ldots, S_p$ as coordenadas em $\mathbb{A}^p$ e $T_1, \ldots, T_q$ as coordenadas em $\mathbb{A}^q$ de tal forma que as restrições de $s_1, \ldots, s_p$ geram $\mathbb{K}(X)$ e as restrições de $t_1, \ldots, t_q$ geram $\mathbb{K}(Y)$. Desse conjunto gerador é possível extrair bases de transcendencia: $s_1, \ldots, s_n$ e

$t_1, \ldots, t_m$. Como $\mathbb{K}(X \times Y) = \mathbb{K}(s_1, \ldots, s_p, t_1, \ldots, t_q)$ e $\mathbb{K}(s_1, \ldots, s_p, t_1, \ldots, t_q)$ é uma extensão algébrica de $\mathbb{K}(s_1, \ldots, s_n, t_1, \ldots, t_m)$, basta mostrar que $\mathbb{K}(s_1, \ldots, s_n, t_1, \ldots, t_m)$ é puramente transcendente sobre $\mathbb{K}$. Suponha que exista uma relação polinomial $f(s_1, \ldots, s_m, t_1, \ldots, t_n) = 0$. Então, para cada $x = (x_1, \ldots, x_p) = (s_1(x), \ldots, s_p(x)) \in X$, a função polinomial dada por $f(x_1, \ldots, x_m, t_1, \ldots, t_n)$ é zero em todo Y. A independência algébrica do conjunto $\{t_1, \ldots, t_n\}$ faz com que todos os coeficientes $g(x_1, \ldots, x_m)$ de $f(x_1, \ldots, x_m, T_1, \ldots, T_n)$ sejam zero. A independência algébrica do conjunto $\{s_1, \ldots, s_m\}$ faz com que $g(S_1, \ldots, S_m) = 0$. Isso significa que $f = 0$ e portanto $\mathbb{K}(s_1, \ldots, s_n, t_1, \ldots, t_m)$ é puramente transcendente sobre $\mathbb{K}$. $\square$

Proposição 3.2.6. Sejam X uma variedade irredutível e $Y \subseteq X$ uma subvariedade irredutível. Então:

(i) $\dim(Y) \leq \dim(X)$.

(ii) $X = Y$, quando $\dim(Y) = \dim(X)$.

Dem: (i) Sem perda de generalidade, assuma que X é uma variedade afim de dimensão d e Y uma subvariedade afim, irredutível e própria de X, cujo ideal associado é P, $P \neq \{0\}$. Uma base de transcendência para $\mathbb{K}(X)$ pode ser obtida em $\mathbb{K}[X]$ e uma base de transcendência para $\mathbb{K}(Y)$ pode ser obtida em $\mathbb{K}[Y]$. Suponha que $\dim Y \geq d$ e tome $x_1, \ldots, x_d \in \mathbb{K}[X]$ elementos algebricamente independentes tais que suas imagens $\overline{x_1}, \ldots, \overline{x_d}$ sejam também algebricamente independentes em $\mathbb{K}[X]/P$. Considere agora, um polinômio não nulo $f \in P$. Como $\dim X = d$, existe uma relação algébrica $g(f, x_1, \ldots, x_d)$, onde $g(T_0, \ldots, T_d) \in \mathbb{K}[T]$. Como $f \neq 0$, T_0 não divide todos os monômios de g e $h(T_1, \ldots, T_d) = g(0, T_1, \ldots, T_d) \neq 0$. Isso implica que $h(\overline{x_1}, \ldots, \overline{x_d}) = 0$, o que é um absurdo, pois contradiz o fato de $\overline{x_1}, \ldots, \overline{x_d}$ serem algebricamente independentes.

(ii) A prova deste item é imediata da prova do item anterior.

$\square$

Para toda subvariedade irredutível Y de uma variedade irredutível X, podemos definir sua *codimensão* como $codim_X Y = \dim(X) - \dim(Y)$. Pela primeira afirmação da proposição anterior, sabemos que $codim_X Y \geq 0$.

Um corolário desta proposição é que as subvariedades de codimensão 1 são de certa forma maximais.

Corolário 3.2.7. Se X é uma variedade afim irredutível e $Y \subseteq X$ é uma subvariedade irredutível de codimensão 1 então Y é uma componente irredutível de alguma variedade $V(\langle f \rangle)$, $f \in \mathbb{K}[X]$.

Dem: Como a codimensão de Y é 1, $Y \subsetneq X$. Por isso, existe um polinômio $f \in \mathbb{K}[X] \setminus \{0\}$ que anula Y, de tal forma que $Y \subseteq V(\langle f \rangle) \subsetneq X$. Considere Z uma componente irredutível de $V(\langle f \rangle)$ que contém Y. Pela proposição anterior, $\dim Y \leq \dim Z < \dim X$. Como a codimensão de Y é 1, $\dim Y = \dim Z$ e, pela proposição anterior, $Y = Z$. $\square$

Definição 3.2.8. Define-se uma *hipersuperfície* como uma variedade afim da forma $X = V(f)$ para algum polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$.

Nesses termos, o que o corolário anterior afirma é que se a subvariedade irredutível afim Y da variedade irredutível afim X tem codimensão 1 então Y é uma componente irredutível de uma hipersuperfície de X. As perguntas naturais são as seguintes. Vale a volta? Quais são as componentes irredutíveis de uma hipersuperfície ? Toda componente irredutível de uma hipersuperfície é uma subvariedade irredutível de codimensão 1 ?

Considere, primeiro, o caso particular em que $X = \mathbb{A}^n$:

Proposição 3.2.9. Toda componente irredutível de uma hipersuperfície em $\mathbb{A}^n$ é uma subvariedade de codimensão 1 em $\mathbb{A}^n$.

Dem: Sem perda de generalidade, assuma $X = V(p)$ onde $p(T) \in \mathbb{K}[x_1, \ldots, x_n]$ é um polinômio irredutível. Sem perda de generalidade, assuma que a variável T_n ocorra de fato em $p(T)$. Considere t_i a restrição de T_i para cada $i = 1, \ldots, n$ de modo que $\mathbb{K}(X) \simeq \mathbb{K}(t_1, \ldots, t_n)$. Se for mostrado que $t_1, \ldots, t_{n-1}$ são algebricamente independentes sobre $\mathbb{K}$, então obtem-se que $\dim X = n - 1$, ou seja, a codimensão de X é 1. Suponha que $t_1, \ldots, t_{n-1}$ não são algebricamente independentes, ou seja, existe uma relação algébrica $g(t_1, \ldots, t_{n-1}) = 0$. Nesse caso, g anula X e como $I(X) = \langle p \rangle$, $g \in \langle p \rangle$. Isso é um absurdo porque T_n ocorre em p, mas não ocorre em g. $\square$

Agora, o caso geral:

Teorema 3.2.10. Sejam X uma variedade afim irredutível, $f \in \mathbb{K}[X]$ um polinômio não constante e Y uma componente irredutível de $V(\langle f \rangle)$. Então Y tem codimensão 1 em X.

Dem: [Hum2], p.27. $\square$

Do teorema anterior conclui-se que, para toda variedade irredutível afim X e toda função regular num aberto $U \subseteq X$, $f \in \mathcal{O}_X(U)$, se f não for uma unidade então as componentes irredutíveis de $V(\langle f \rangle)$ têm codimensão 1 em X.

Outro corolário do teorema anterior é:

Corolário 3.2.11. Sejam X uma variedade irredutível e Y uma subvariedade irredutível de X. Se $codim_X Y = r$ então existe uma cadeia de subvariedades irredutíveis $X \supset Y_1 \supset \ldots \supset Y_{r-1} \supset Y$ satisfazendo $codim_X Y_i = i$, $\forall\, i = 1, \ldots, r-1$. Em particular, existem variedades irredutíveis de quaisquer codimensões dentro de X.

Dem: Basta considerar o caso em que X é afim. O caso $r = 1$ já foi mostrado no corolário 3.2.7. O caso geral será provado usando indução em r. Como $Y \subsetneq X$ existe uma função não nula $f \in I(Y)$ e $Y \subseteq Y_1$, onde Y_1 é uma componente irredutível de $V(\langle f \rangle)$. Pelo teorema 3.2.10 $codim_X Y_1 = 1$. Usando a hipótese de indução em Y_1, obtem-se o resultado. $\square$

É possível redefinir a dimensão de uma variedade irredutível X como sendo o maior comprimento de uma cadeia estritamente decrescente de subvariedades irredutíveis em X.

Definição 3.2.12. Seja X uma variedade irredutível. Defina a *dimensão* de X como o supremo de todos os inteiros para os quais existe uma cadeia estritamente decrescente de subvariedades irredutíveis de X de tal comprimento.

A seguinte proposição é corolário do teorema 3.2.10.

Proposição 3.2.13. Seja X uma variedade irredutível. Toda subvariedade $V(f_1, \ldots, f_r) \subset X$, com $\{f_1, \ldots, f_r\} \subset \mathcal{O}_X(X)$, tem codimensão menor ou igual a r.

3.3 Espaços tangentes

Nesta seção, o objetivo é definir o espaço tangente, principalmente para variedades afins. Será nesse caso que a seção focará, pois ele será usado no capítulo seguinte. Considere $\mathbb{K}$ um corpo algebricamente fechado.

A ideia é definir o espaço tangente em um ponto de uma variedade de forma algébrica, intrínseca e de tal forma que a definição seja compatível com as definições usuais de geometria diferencial. Ou seja, definir o espaço tangente em um ponto de tal forma que os vetores tangentes representem as tangentes às curvas que passam por tal ponto. Como toda variedade é colagem de variedades afins, é conveniente começar definindo espaços tangentes de curvas afins.

Seja $C = V(\langle f \rangle) \subset \mathbb{A}^2$ para algum $f \in \mathbb{C}[x, y]$. Pelo teorema da função implícita, para todo ponto $(a, b) \in C$ em que o gradiente é não nulo, ou seja, $(\partial_x f(a, b), \partial_y f(a, b)) \neq (0, 0)$, a curva C é o gráfico de uma função : $\mathbb{A}^1 \to \mathbb{A}^1$. Nesse caso, define-se o espaço tangente a C no ponto (a, b) como

$$T_{(a,b)}C = V(\langle \partial_x f(a, b)(x - a) + \partial_y f(a, b)(y - b) \rangle).$$

O que foi feito para obter o espaço tangente em um ponto (a, b) numa curva plana afim $C = V(\langle f \rangle)$ foi escrever a expansão em série de Taylor do polinômio f em torno de (a, b). Assim obtem-se $f = f_0 + f_1 + \ldots + f_d$, onde d é o grau do polinômio f e para cada $k = 1, \ldots, d$,

$$f_k = \frac{1}{k!} \sum_{i+j=k} \frac{\partial^k f}{\partial x^i y^j}(a, b)(x - a)^i (y - b)^j.$$

Como (a, b) pertence a curva $V(\langle f \rangle)$, $f_0 = 0$. Defina então

$$T_{(a,b)}C = V(\langle f_1 \rangle).$$

Em outras palavras, $T_{(a,b)}C$ é a variedade afim associada a linearização de f.

Seguindo esta ideia, defina para cada $f \in \mathbb{K}[x_1, \ldots, x_n]$ e cada ponto $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$, a linearização de f em torno de a como

$$d_a f = \partial_1 f(a)(x_1 - a_1) + \ldots + \partial_n f(a)(x_n - a_n).$$

Desta forma, para qualquer variedade afim $X = V(\langle f \rangle)$, $f \in \mathbb{K}[x_1, \ldots, x_n]$, define-se o espaço tangente a X em cada ponto $a \in V(\langle f \rangle)$ como

$$T_a X = V(\langle d_a f \rangle).$$

Toda variedade afim é da forma $X = V(I)$, onde I é um ideal de $\mathbb{K}[x_1, \ldots, x_n]$. Como $V(I) = \cap_{j=1}^m V(\langle f_j \rangle)$, para toda variedade afim, o espaço tangente rm um ponto $a \in X$ pode ser definido como

$$T_a X = \bigcap_{j=1}^m V(\langle d_a f_j \rangle).$$

Isso define o espaço tangente rm um ponto de uma variedade afim qualquer.

Para cada ponto p de uma variedade X existem abertos afins U_i que contém p. Escolha um tal aberto afim e defina o espaço tangente a X em p como o espaço tangente $T_p(U_i)$.

Definido desta forma, o espaço tangente a uma variedade num ponto é uma outra variedade. Esta definição, no entanto não é intrínseca, já que depende da escolha de aberto afim em torno de cada ponto. Por isso é conveniente procurar outra definição.

Definição 3.3.1. Sejam X uma variedade afim irredutível munida do feixe estrutural $\mathcal{O}_X$ e p um ponto em X. As derivadas da variedade X no ponto p são as derivações pontuais do anel de funções regulares de X, ou seja, o conjunto de transformações lineares $\delta : \mathcal{O}_X(X) \to \mathbb{K}$ satisfazendo

$$\delta(fg) = f(p)\delta(g) + \delta(f)g(p), \quad \forall\, f, g \in \mathcal{O}_X(X).$$

Para determinar as derivações pontuais do anel $\mathcal{O}_X(X)$, basta determinar como a derivação age no conjunto

$$I_p = \{f : \mathcal{O}_X(X) \to \mathbb{K} \mid f(p) = 0\}.$$

De fato, se $f \in \mathcal{O}_X(X)$ e $f(p) \neq 0$, isto é, se $f \notin I_p$, então $g = f - f(p) \in I_p$ e $d(g) = d(f) - d(f(p)) = d(f)$ para toda d, derivação pontual de $\mathcal{O}_X(X)$, porque $f(p) \in \mathbb{K}$.

Além disso, se $h \in \mathcal{O}_X(X)$ e h é escrito da forma $h = fg$, onde $f, g \in I_p$, isto é, se $h \in (I_p)^2$, então para toda d, derivação pontual de $\mathcal{O}_X(X)$, $d(h) = f(p)d(g) + d(f)g(p)$. Como $f(p) = g(p) = 0$, então $d(h) = 0$. Assim, a cada derivação pontual de $\mathcal{O}_X(X)$ é possível associar um único elemento no espaço dual de $I_p/(I_p)^2$ (sobre o corpo $\mathcal{O}_X(X)/I_p$).

Considere X uma variedade qualquer munida do feixe $\mathcal{O}_X$ e p um ponto de X. Por definição, existe um aberto afim $U \subseteq X$ que contém p. Considerando o anel de funções regulares $\mathcal{O}_X(U)$, é possível definir o espaço tangente a X no ponto p como as derivações pontuais de $\mathcal{O}_X(U)$. Para evitar arbitrariedade na escolha do aberto afim, basta considerar o anel local $\mathcal{O}_p$ em lugar de $\mathcal{O}_X(U)$ e o ideal maximal $\mathfrak{m}_p = \{f : \mathcal{O}_p \to \mathbb{K} \mid f(p) = 0\}$ em lugar de I_p.

Definição 3.3.2. Sejam X uma variedade algébrica irredutível e p um ponto de X. Sejam $\mathcal{O}_{X,p}$ o anel local de funções regulares de X no ponto p e $\mathfrak{m}_{X,p}$ o único ideal maximal de $\mathcal{O}_{X,p}$. Define-se o espaço tangente a variedade X no ponto p como

$$T_pX = (\mathfrak{m}_{X,p}/\mathfrak{m}_{X,p}{}^2)^*.$$

Observe que as derivações de $\mathbb{K}[x_1, \dots, x_n]$ são geradas pelas derivadas $\{\partial_1, \dots, \partial_n\}$. Portanto esta definição coincide com a definição intuitiva dada inicialmente.

Proposição 3.3.3. Sejam X e Y duas variedades irredutíveis, $x \in X$ e $y \in Y$. Então: $T_{(x,y)}(X \times Y) \simeq T_xX \bigoplus T_yY$.

Dem: Usando a definição acima, basta ver que $\mathcal{O}_{(x,y)}$ é a localização de $\mathcal{O}_x \otimes \mathcal{O}_y$ pelo ideal maximal $\mathfrak{m}_x \otimes \mathcal{O}_y + \mathcal{O}_x \otimes \mathfrak{m}_y$. Usando a proposição 3.1.36, obtem-se o resultado. □

Definição 3.3.4. Sejam X uma variedade algébrica e $p \in X$. Diz-se que o ponto p é *regular* quando a dimensão do espaço tangente à X no ponto p é igual a dimensão da variedade X, ou seja,

$$\dim_{(\mathcal{O}_p/\mathfrak{m}_p)} T_pX = \dim X.$$

Um ponto que não é regular é dito *singular*. Uma variedade é dita *suave* quando todos os seus pontos são regulares.

Exemplo 3.3.5.

(i) Para todo ponto $p \in \mathbb{A}^n$, $T_p\mathbb{A}^n \simeq \mathbb{A}^n$, pois as derivações de $\mathbb{K}[x_1, \dots, x_n]$ são geradas por $\{\partial_1, \dots, \partial_n\}$. Analogamente, para todo ponto $p \in \mathbb{P}^n$, $T_p\mathbb{P}^n \simeq \mathbb{A}^n$. Portanto, todos os pontos dos espaços afins e projetivos são regulares e estas variedades são suaves.

(ii) Considere o aberto principal $Gl_n(\mathbb{K})$ e a identidade do grupo $e \in Gl_n(\mathbb{K})$. O anel local $\mathcal{O}_e$ é isomorfo a localização de $\mathbb{K}[Gl_n]$ pelo ideal maximal $\langle x_{ij} - \delta_{ij} : 1 \leq i,j \leq n \rangle$ e o ideal maximal $\mathfrak{m}_e$ é dado pelas funções racionais $f/g \in \mathcal{O}_e$, tais que $f(e) = 0$. Portanto ${\mathfrak{m}_e}^2$ é dado pelas funções racionais $f_1 f_2/g \in \mathcal{O}_e$, tais que $f_1(e) = f_2(e) = 0$.

   Como $\mathfrak{m}_e = \langle x_{ij} - \delta_{ij} : 1 \leq i,j \leq n \rangle$, o espaço tangente a $Gl_n(\mathbb{K})$ é o conjunto de funcionais lineares em $\langle x_{ij} - \delta_{ij} : 1 \leq i,j \leq n \rangle^*$ que se anulam em $\langle x_{ij} - \delta_{ij} : 1 \leq i,j \leq n \rangle^2$. Esse conjunto de funcionais pode ser gerado pelos funcionais x_{ij} que associam o valor 1 ao polinômio $(x_{ij} - \delta_{ij})$ e 0 a todos os outros polinômios de $\mathcal{O}_e$.

   Identificando os funcionais x_{ij} com os elementos e_{ij} da base canônica das matrizes de ordem n, obtem-se que o espaço tangente a $Gl_n(\mathbb{K})$ na identidade é isomorfo ao espaço de matrizes de ordem n, $T_e(Gl_n(\mathbb{K})) \simeq \mathfrak{gl}_n$.

(iii) De forma análoga ao exemplo anterior: o espaço tangente a $T_n(\mathbb{K})$ é isomorfo a $\mathfrak{t}_n(\mathbb{K})$, o espaço tangente a $U_k(\mathbb{K})$ é isomorfo a $\mathfrak{n}_k(\mathbb{K})$ e o espaço tangente a $D_n(\mathbb{K})$ é isomorfo a $\mathfrak{d}_n(\mathbb{K})$.

Teorema 3.3.6. Para todo ponto p numa variedade irredutível X, $\dim(T_pX) \geq \dim X$. Além disso, o conjunto de pontos regulares de X é um aberto (denso).

Dem: [Hum2], p.40. □

Considere X uma variedade irredutível munida do feixe $\mathcal{O}_X$ e p um ponto de X. Usando o Lema de Nakayama (1.2.28), o ideal maximal $\mathfrak{m}_p$ é gerado por $\{f_1, \ldots, f_k\}$ se, e somente se, o espaço vetorial $(T_pX)^*$ for gerado por $\{\overline{f_1}, \ldots, \overline{f_k}\}$. Consequentemente, por um lado, o número mínimo de geradores para $\mathfrak{m}_p$ é a dimensão de X e, por outro lado, o conjunto $\{f_1, \ldots, f_k\}$ é algebricamente independente.

É natural se perguntar se um morfismo entre variedades induz um morfismo entre os espaços tangentes. Ou seja, se dados $\varphi : X \to Y$ um morfismo entre variedades irredutíveis e p um ponto de X, existe naturalmente uma transformação linear $\psi : T_pX \to T_{\varphi(p)}Y$. Tal transformação linear deve associar um elemento $\psi(\mathsf{x})$ em $(\mathfrak{m}_{Y,\varphi(p)}/{\mathfrak{m}_{Y,\varphi(p)}}^2)^*$ a cada elemento x em $(\mathfrak{m}_{X,p}/{\mathfrak{m}_{X,p}}^2)^*$. Como o comorfismo φ^* induz um morfismo $\varphi_p^* : \mathcal{O}_{Y,\varphi(p)} \to \mathcal{O}_{X,p}$, é natural a seguinte definição.

Definição 3.3.7. Sejam $\varphi : X \to Y$ um morfismo entre variedades irredutíveis e p um ponto de X. Defina o *diferencial de φ em p* como a transformação linear entre os espaços vetoriais tangentes $d_p\varphi : T_pX \to T_{\varphi(p)}Y$, tal que, para todo $\mathsf{x} \in T_pX$, $d_p\varphi(\mathsf{x}) = \mathsf{x} \circ \varphi^* \in T_{\varphi(p)}Y$.

Proposição 3.3.8. Sejam $\varphi : X \to Y$ e $\psi : Y \to Z$ morfismos entre variedades irredutíveis, $x \in X$ e $y = \varphi(x) \in Y$. Então:

(i) $d_x(id_X) = id_{T_xX}$;

(ii) $d_x(\psi \circ \varphi) = d_y\psi \circ d_x\varphi$.

Dem:

(i) Por definição, para cada $\mathsf{x} \in T_xX$, $d_x id_X(\mathsf{x}) = \mathsf{x} \circ id_X^*$. Como $id_X^* = id_{\mathcal{O}_X(X)}$, $d_x id_X(\mathsf{x}) = \mathsf{x}$.

(*ii*) Para cada $\mathsf{x} \in T_xX$, $d_x\varphi(\mathsf{x}) = \mathsf{x} \circ \varphi^* \in T_yY$. Para cada $\mathsf{y} \in T_yY$, $d_y\psi(\mathsf{y}) = \mathsf{y} \circ \psi^*$, em particular, $d_y\psi(\mathsf{x} \circ \varphi^*) = (\mathsf{x} \circ \varphi^*) \circ \psi^* = \mathsf{x} \circ (\varphi^* \circ \psi^*) = \mathsf{x} \circ (\psi \circ \varphi)^* = d_x(\psi \circ \varphi)(\mathsf{x})$. Portanto $d_y\psi \circ d_x\varphi = d_x(\psi \circ \varphi)$.

$\square$

Exemplo 3.3.9.

(*i*) Seja $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ um morfismo de variedades afins linear. Assim como existe uma identificação entre $T_p\mathbb{A}^n$ e $\mathbb{A}^n$, existe uma identificação entre $d_p\varphi$ e φ. Sem perda de generalidade, basta considerar o caso em que $p = 0$. Se φ é um morfismo linear, para cada $(x_1, \ldots, x_n) \in \mathbb{A}^n$,

$$\varphi(x_1, \ldots, x_n) = \left(\sum_{j=1}^{n} \varphi_{1j}x_j, \ldots, \sum_{j=1}^{n} \varphi_{nj}x_j \right)$$

para alguns $\varphi_{ij} \in \mathbb{K}$. Agora considere $\mathsf{x} \in T_0\mathbb{A}^n \simeq (\mathfrak{m}_0/{\mathfrak{m}_0}^2)^*$. Pela identificação entre $T_0\mathbb{A}^n$ e $\mathbb{A}^n$, x é identificado com $(a_1, \ldots, a_n)$, onde $a_i = \mathsf{x}(x_i)$. Usando esta identificação,

$$\begin{aligned} d_0\varphi(\mathsf{x})(x_i) &= \mathsf{x}(\varphi^*(x_i)) \\ &= \mathsf{x}\left(\sum_{j=1}^{n} \varphi_{ij}x_j \right) \\ &= \sum_{j=1}^{n} \varphi_{ij}\mathsf{x}(x_j) \\ &= \sum_{j=1}^{n} \varphi_{ij}a_j. \end{aligned}$$

Portanto $d_0\varphi(a_1, \ldots, a_n) = \left(\sum_{j=1}^{n} \varphi_{1j}a_j, \ldots, \sum_{j=1}^{n} \varphi_{nj}a_j \right)$ para todo $(a_1, \ldots, a_n) \in \mathbb{A}^n$ e $d_0\varphi$ pode ser identificado com φ.

(*ii*) Sejam $e = id_n$ (a matriz identidade de ordem n), A uma matriz de ordem n com entradas $a_{ij} \in \mathbb{K}$ e o morfismo $\det : Gl_n(\mathbb{K}) \to \mathbb{A}^1$. O diferencial do determinante é o traço, ou seja, $d_e(\det)(A) = Tr(A)$.

(*iii*) Usando o exemplo anterior e o exemplo 3.3.5 (*ii*), obtem-se que o espaço tangente à variedade $Sl_n(\mathbb{K})$ é isomorfo ao conjunto de matrizes de ordem n e traço zero. Ou seja, $T_eSl_n(\mathbb{K}) \simeq \mathfrak{sl}_n$.

Sejam X uma variedade afim sobre $\mathbb{K}$ e $x \in X$. Considere o ideal maximal das funções regulares em X que anulam o ponto x, $I_x = \{f \in \mathbb{K}[X] \mid f(x) = 0\}$. Observe que $\mathbb{K}[X] \simeq \mathbb{K} \oplus I_x$. De fato, para toda $f \in \mathbb{K}[X]$, a função $f_0 = f - f(x)$ também é regular e pertence a I_x. Por outro lado, para toda função regular $f \in I_x$ e para todo $k \in \mathbb{K}$, a função definida por $f_1(a) = f(a) + k$ é regular.

Levando em conta estas observações e a definição de espaço tangente, é natural considerar a seguinte definição:

Definição 3.3.10. Sejam X uma variedade afim sobre $\mathbb{K}$ e $x \in X$. Defina o espaço de *distribuições de ordem* $\leq n$ *em* X *com suporte em* x como

$$D_n(X, x) = \{\varphi \in \mathbb{K}[X]^* \mid \varphi(I_x^{n+1}) = 0\}.$$

Defina, analogamente, o espaço de *distribuições de ordem* $\leq n$ *em* X *com suporte em* x *sem termo constante* como

$$D_n^+(X, x) = \{\varphi \in D_n(X, x) \mid \varphi(1_{\mathbb{K}[X]}) = 0\},$$

onde $1_{\mathbb{K}[X]}$ é a função regular em X que associa a todo ponto $x \in X$, $1(x) = 1 \in \mathbb{K}$.

Defina o espaço de *distribuições em* X *com suporte em* x como

$$D(X, x) = \bigcup_{n \in \mathbb{N}} D_n(X, x).$$

Analogamente, defina o espaço de *distribuições em* X *com suporte em* x *sem termo constante* como

$$D^+(X, x) = \bigcup_{n \in \mathbb{N}} D_n^+(X, x).$$

Usando a definição 1.3.13, é equivalente definir $D_n(X, x)$ como a álgebra dual finita de $\mathbb{K}[X]$ com relação ao ideal ${I_x}^{n+1}$, para cada $n \in \mathbb{N}$. Desta forma, o espaço das distribuições de ordem n com suporte em x tem estrutura de coálgebra. Analogamente, como $D_0(X, x) \supseteq D_1(X, x) \supseteq \ldots \supseteq D_n(X, x) \supseteq \ldots$, o espaço das distribuições em X com suporte em x também têm estrutura de coálgebra.

Proposição 3.3.11.

(i) Para cada $n \in \mathbb{N}$, $D_n(X, x)$ é isomorfo ao espaço vetorial dual a $(\mathbb{K}[X]/I_x^{n+1})$. Em particular, $D_0(X, x) \simeq \mathbb{K}^* \simeq \mathbb{K}$.

(ii) Para cada $n \in \mathbb{N}$, $D_n(X, x) = \mathbb{K} \oplus D_n^+(X, x)$.

(iii) Para cada $n \in \mathbb{N}^\bullet$, existe um isomorfismo natural entre $D_n^+(X, x)$ e $(I_x/I_x^{n+1})^*$ como espaços vetoriais. Em particular, $D_1^+(X, x) \simeq T_x X$.

Dem:

(i) Se $f \in \mathbb{K}[X]^*$ e $\ker(f) \supseteq I_x^{n+1}$, então existe $\overline{f} \in (\mathbb{K}[X]/I_x^{n+1})^*$, tal que $\overline{f} \circ \pi = f$, onde $\pi : \mathbb{K}[X] \to \mathbb{K}[X]/I_x^{n+1}$ é a projeção canônica. Defina o morfismo linear que associa a cada $f \in \mathbb{K}[X]^*$ o funcional $\overline{f} \in (\mathbb{K}[X]/I_x^{n+1})^*$ como acima. Esta transformação linear é sobrejetiva, porque, para cada $g \in (\mathbb{K}[X]/I_x^{n+1})^*$, é possível definir um funcional linear $\tilde{g} \in \mathbb{K}[X]^*$, tal que $\tilde{g}(\varphi) = g(\pi(\varphi))$. Para mostrar a injetividade, considere $f \in \mathbb{K}[X]$, tal que $\overline{f}(\varphi) = 0$ para todo $\varphi \in (\mathbb{K}[X]/I_x^{n+1})^*$. Isso implica que $f = 0 \in \mathbb{K}[X]^*$.

(ii) Para cada $n \in \mathbb{N}$, considere um funcional $f \in D_n(X, x)$, tal que $f(1) = a$, onde $1 = 1_{\mathbb{K}}$. Considere o funcional $g = f - a \in D_n(X, x)$. Por definição, $g(1) = f(1) - a = 0$. Portanto $g \in D_n^+(X, x)$ e é possível escrever f como soma de $g \in D_n^+(X, x)$ e $a \in \mathbb{K}$. Agora considere um funcional $f \in D_n^+(X, x) \cap \mathbb{K}$. Isso significa que $f(1) = 0$. Consequentemente $f = 0$.

(iii) Esse item é imediato dos itens anteriores.

$\square$

Exemplo 3.3.12.

(i) Considere o espaço afim $\mathbb{A}^1$ e o ponto $0 \in \mathbb{A}^1$. O anel de funções regulares de $\mathbb{A}^1$ é isomorfo a $\mathbb{K}[x]$ e o ideal $I_0 = \langle x \rangle \subseteq \mathbb{K}[x]$.

O espaço dual a $\mathbb{K}[\mathbb{A}^1]$ é o espaço de transformações lineares $Hom_{\mathbf{Mod}_{\mathbb{K}}}(\mathbb{K}[x], \mathbb{K})$. Então $\mathbb{K}[\mathbb{A}^1]^*$ é o espaço de séries formais de funcionais lineares $x_i \in \mathbb{K}[x]^*$, definidos por

$$x_i(x^j) = \delta_{ij}, \quad i, j \in \mathbb{N}.$$

O conjunto das distribuições de $\mathbb{A}^1$ com suporte no ponto 0 é portanto

$$\{f \in \mathbb{K}[x]^* \mid \exists\ m \in \mathbb{N},\ f(x^{m+1}) = 0\},$$

ou seja, $D(\mathbb{A}^1, 0)$ é o $\mathbb{K}$-espaço vetorial gerado pelos funcionais x_i, $i \in \mathbb{N}$.

Como a multiplicação da álgebra de funções regulares $\mathbb{K}[x]$ é dada pela multiplicação usual de polinômios, a comultiplicação em $D(\mathbb{A}^1, 0)$, denotada por Δ_d, é, por um lado,

$$\begin{aligned} \Delta_d(x_k)(x^n \otimes x^m) &= \sum_{0 \leq i,j} c_{ij,k} x_i(x^n) x_j(x^m) \\ &= c_{nm,k} \end{aligned}$$

para alguns $c_{ij,k} \in \mathbb{K}$ e, por outro lado,

$$\begin{aligned} \Delta_d(x_k)(x^n \otimes x^m) &= x_k \circ \mu(x^n \otimes x^m) \\ &= \delta_{k,n+m}, \end{aligned}$$

para todo $k, m, n \in \mathbb{N}$. Portanto:

$$\Delta_d(x_k) = \sum_{0 \leq l \leq k} x_l \otimes x_{k-l}, \quad k \in \mathbb{N}.$$

Como a unidade da álgebra de funções regulares $\mathbb{K}[x]$ é dada pela identificação do corpo $\mathbb{K}$ em $\mathbb{K}[x]$, a counidade de $D(\mathbb{A}^1, 0)$ é dada por

$$\begin{aligned} \varepsilon_d(x_n)(k) &= x_n \circ u(k) \\ &= k\delta_{n,0}, \end{aligned}$$

para todo $k \in \mathbb{K}$. Portanto

$$\varepsilon_d(x_0) = 1 \quad e \quad \varepsilon_d(x_n) = 0, \quad n \in \mathbb{N}^{\bullet}.$$

(Vendo os elementos de $D(\mathbb{A}^1, 0)$ como polinômios em x_i, a counidade representa a avaliação desses polinômios no zero. A imagem é o “coeficiente livre do polinômio”.)

(*ii*) Considere o aberto principal $(\mathbb{A}^1)^\bullet$ e o ponto $1 \in (\mathbb{A}^1)^\bullet$. O anel de funções regulares de $(\mathbb{A}^1)^\bullet$ é isomorfo a $\mathbb{K}[t, t^{-1}]$ e o ideal $I_1 = \langle x-1 \rangle$.

O espaço dual a $\mathbb{K}[(\mathbb{A}^1)^\bullet]$ é o espaço de transformações lineares $Hom_{\mathbf{Mod}_\mathbb{K}}(\mathbb{K}[t, t^{-1}], \mathbb{K})$. Logo $\mathbb{K}[(\mathbb{A}^1)^\bullet]^*$ é o espaço de séries formais de funcionais $t_i \in \mathbb{K}[t, t^{-1}]^*$ definidos por

$$t_i((t^j - 1)) = \delta_{ij},$$

para cada $i, j \in \mathbb{Z}$. As distribuições de $(\mathbb{A}^1)^\bullet$ são portanto

$$\{f \in \mathbb{K}[t, t^{-1}]^* \mid \exists\, m \in \mathbb{N},\ f((t-1)^{m+1}) = 0\},$$

ou seja, $D((\mathbb{A}^1)^\bullet, 1)$ é o $\mathbb{K}$-espaço vetorial gerado pelos funcionais t_i, $i \in \mathbb{N}$.

De fato, não se precisa dos funcionais t_j, $j < 0$, pois para cada $m \in \mathbb{N}$, o polinômio $(t^{-1} - 1)$, visto como elemento de $\mathbb{K}[t, t^{-1}]/I_1^{m+1}$, pode ser escrito como combinação linear de $(t-1)^k$, com $0 < k \leq m$. Isso ocorre, porque, como elemento de $\mathbb{K}[t, t^{-1}]/I_1^{m+1}$, $(t^{-1} - 1)(t-1)^m = 0$. Desenvolvendo a m-ésima potência de $(t-1)$, obtem-se:

$$\begin{aligned} 0 &= t^{-1} \left(\sum_{0 \leq n \leq m} \binom{m}{n} (-1)^{m-n} t^n \right) - (t-1)^m \\ &= (-1)^m t^{-1} + \left(\sum_{1 \leq n \leq m} \binom{m}{n} (-1)^{m-n} t^{n-1} \right) - (t-1)^m. \end{aligned}$$

Portanto

$$t^{-1} = \left(\sum_{1 \leq n \leq m} \binom{m}{n} (-t)^{n-1} \right) + (1-t)^m.$$

Isso faz com que o funcional t_{-1} também possa ser escrito como combinação linear de $\{t_k \mid k \in \mathbb{N}\}$ em $D((\mathbb{A}^1)^\bullet, 1)$. O resultado para os outros funcionais t_k, $k < 0$, segue de forma análoga.

Como a multiplicação da álgebra de funções regulares $\mathbb{K}[t, t^{-1}]$ é dada pela multiplicação usual de polinômios de Laurent, a comultiplicação em $D((\mathbb{A}^1)^\bullet, 1)$, denotada por Δ_d, é dada por um lado por

$$\begin{aligned} \Delta_d(t_k)((t-1)^n \otimes (t-1)^m) &= \sum_{0 \leq i,j} c_{ij} t_i((t-1)^n) t_j((t-1)^m) \\ &= c_{nm} \end{aligned}$$

para alguns $c_{ij} \in \mathbb{K}$ e por outro lado, por

$$\begin{aligned} \Delta_d(t_k)((t-1)^n \otimes (t-1)^m) &= t_k \circ \mu((t-1)^n \otimes (t-1)^m) \\ &= t_k((t-1)^{n+m}) \\ &= \delta_{k,n+m}, \end{aligned}$$

para todo $k, n, m \in \mathbb{N}$. Portanto

$$\Delta_d(t_k) = \sum_{0 \leq l \leq k} t_l \otimes t_{k-l}, \quad \forall\, k \in \mathbb{N}.$$

Como a unidade da álgebra de funções regulares $\mathbb{K}[t, t^{-1}]$ é dada pela identificação do corpo $\mathbb{K}$ na álgebra de polinômios de Laurent, a counidade de $D((\mathbb{A}^1)^\bullet, 1)$ é dada por

$$\begin{aligned}\varepsilon_d(t_i)(k) &= t_i \circ u(k)\\ &= k\delta_{i,0},\end{aligned}$$

para todo $i \in \mathbb{N}$ e para todo $k \in \mathbb{K}$. Ou seja,

$$\varepsilon_d(t_0) = 1 \quad e \quad \varepsilon_d(t_i) = 0, \quad i \in \mathbb{N}^\bullet.$$

(Vendo os elementos de $D((\mathbb{A}^1)^\bullet, 1)$ como polinômios em t_i, a counidade representa a avaliação desses polinômios no zero. A imagem é o "coeficiente livre do polinômio".)

(iii) Considere o aberto principal $Gl_2(\mathbb{K}) \subseteq \mathbb{A}^4$. Como descrito no exemplo 3.1.35 (ii), o anel de funções regulares de $Gl_2(\mathbb{K})$ é isomorfo ao anel de funções regulares da subvariedade fechada de $\mathbb{A}^5$ definida pelo ideal $\langle d(xw - yz) - 1\rangle \subseteq \mathbb{K}[x, y, z, w, d]$. Portanto $\mathbb{K}[Gl_2] \simeq \frac{\mathbb{K}[x,y,z,w,d]}{\langle dxw - dyz - 1\rangle}$.

O espaço dual a $\mathbb{K}[Gl_2]$ é o espaço de transformações lineares $Hom_{\mathbf{Mod}_\mathbb{K}}(\mathbb{K}[Gl_2], \mathbb{K})$. Usando a condição $d(xw - yz) - 1$, é possível caracterizar $\mathbb{K}[Gl_2]^*$ como o espaço de séries formais de funcionais lineares $x_i y_j z_k w_l \in \mathbb{K}[Gl_2]^*$ que satisfazem

$$x_i y_j z_k w_l((x-1)^{i'} y^{j'} z^{k'} (w-1)^{l'}) = \delta_{i,i'}\delta_{j,j'}\delta_{k,k'}\delta_{l,l'}$$

para quaisquer $i, i', j, j', k, k', l, l' \in \mathbb{N}$.

Considere, agora, a matriz identidade, $id_2 \in Gl_2(\mathbb{K})$. Como descrito no exemplo 3.1.31 (ii), $I_{id_2} = \langle (x-1), y, z, (w-1)\rangle$. Analogamente aos exemplos anteriores, as distribuições de $Gl_2(\mathbb{K})$ com suporte no ponto id_2 são

$$\{f \in \mathbb{K}[Gl_2]^* \mid \exists\, n \in \mathbb{N},\ f(x^i y^j z^k w^l) = 0, \text{ se } i + j + k + l = n + 1\}.$$

Usando a caracterização acima, $D(Gl_2(\mathbb{K}), id_2)$ é o $\mathbb{K}$-espaço vetorial gerado pelo conjunto de funcionais $\{(x_i y_j z_k w_l) \mid i, j, k, l \in \mathbb{N}\}$.

Capítulo 4

Grupos Algébricos

4.1 Definições, exemplos e propriedades

Na presente seção serão feitas algumas definições, dados alguns exemplos e mostradas algumas propriedades sobre grupos algébricos. A estrutura e as demonstrações seguem [Hum2] e [Jan].

Definição 4.1.1. Um *grupo algébrico* é um conjunto X munido de estruturas de variedade algébrica e grupo, tal que a multiplicação do grupo $m : X \times X \to X$; $(x, y) \mapsto xy$ e a inversa $i : X \to X$; $x \mapsto x^{-1}$ são morfismos de variedades.

Observe que o fato da inversa ser um morfismo é equivalente ao fato dela ser um isomorfismo de variedades algébricas. De fato, $i(g^{-1}) = g$, $\forall\ g \in G$. Portanto a inversa é a sua própria inversa.

Os grupos algébricos tratados serão grupos algébricos afins, isto é, grupos algébricos cujas variedades subjacentes são afins. Portanto, a partir daqui, todo grupo algébrico será considerado afim, a menos de menção contrária. Além disso, considere $\mathbb{K}$ como um corpo algebricamente fechado.

As definições de morfismos, isomorfismos, endomorfismos e automorfismos de grupos algébricos são as mais naturais possíveis.

Definição 4.1.2. Um *morfismo* entre grupos algébricos X e Y é uma função de X para Y, que é morfismo de variedades algébricas e homomorfismo de grupos. Um *isomorfismo* entre grupos algébricos é um isomorfismo tanto de variedades algébricas quanto de grupos. Um *endomorfismo* é um morfismo do grupo algébrico nele mesmo, enquanto um *automorfismo* é um isomorfismo do grupo algébrico nele mesmo.

Em um grupo algébrico G é possível definir, para cada $g \in G$, as funções:

(i) $E_g : G \to G$; $E_g : h \mapsto gh$, chamada de *translação à esquerda* por g.

(ii) $D_g : G \to G$; $D_g : h \mapsto hg$, chamada de *translação à direita* por g.

(iii) $C_g : G \to G$; $C_g : h \mapsto ghg^{-1}$, chamada de *conjugação* por g.

Proposição 4.1.3. Em um grupo algébrico, as translações e as conjugações são isomorfismos de variedades. Em particular, todo grupo algébrico é uma variedade suave.

Dem: Considere um grupo algébrico G. Basta mostrar que translações à esquerda são isomorfismos de variedades. De fato, a demonstração é análoga para translações à direita e toda conjugação é composição de translações, a saber, $C_g = D_{g^{-1}} \circ E_g$ para todo $g \in G$.

Como $m : G \times G \to G$ é um morfismo de variedades, $E_g : G \to G$ também é. Além disso, para cada $g \in G$, $E_{g^{-1}}$ é o morfismo inverso de E_g. Portanto, translações à esquerda são automorfismos de variedades algébricas.

As translações também agem transitivamente em G, ou seja, para quaisquer dois elementos $g, h \in G$ existe uma translação cuja imagem de g é h, a saber, $E_{hg^{-1}} : g \mapsto h$. Além disso, como o conjunto de pontos regulares de G é denso, existe um aberto $U \subseteq G$, onde todos os pontos são regulares. Aplicando translações aos elementos de U obtem-se a regularidade de todos os pontos de G. Por esse motivo, todo grupo algébrico é uma variedade suave. □

Exemplo 4.1.4.

(i) Considere o espaço afim $\mathbb{A}^n$ sobre $\mathbb{K}$. Considere $\mathbb{A}^n$ como grupo aditivo com a adição coordenada a coordenada no corpo $\mathbb{K}$. Dessa forma, $\mathbb{A}^n$ é munido de uma estrutura de grupo algébrico. De fato, a multiplicação, $m(x, y) = x + y$, $\forall\ x, y \in \mathbb{A}^n$, é uma função polinomial e a inversa $i(x) = -x$, $\forall\ x \in \mathbb{A}^n$ também. Em particular, a identidade desse grupo algébrico é $(0, \ldots, 0) \in \mathbb{A}^n$.

Considere o caso em que $n = 1$. O espaço afim $\mathbb{A}^1$ é um grupo algébrico chamado de *grupo aditivo* e denotado por $G_a(\mathbb{K})$.

(ii) Considere o espaço afim unidimensional $\mathbb{A}^1$ e seu aberto principal $(\mathbb{A}^1)^\bullet$ sobre $\mathbb{K}$. Considere $(\mathbb{A}^1)^\bullet$ como grupo multiplicativo com multiplicação no corpo $\mathbb{K}$. Dessa forma, $(\mathbb{A}^1)^\bullet$ é munido de uma estrutura de grupo algébrico. De fato, $(\mathbb{A}^1)^\bullet$ é isomorfo a variedade afim, $X = V(\langle xy - 1\rangle) \subseteq \mathbb{A}^2$. A multiplicação $m((x, 1/x), (y, 1/y)) = (xy, 1/xy)$, $\forall\ x, y \in (\mathbb{A}^1)^\bullet$, é uma função polinomial e a inversa $i(x, y) = (y, x)$, $\forall\ x = 1/y \in (\mathbb{A}^1)^\bullet$, também. Em particular, a identidade é o elemento $1 \in (\mathbb{A}^1)^\bullet$. Esse grupo algébrico é chamado de *grupo multiplicativo* e denotado por $G_m(\mathbb{K})$.

(iii) O grupo $Gl_n(\mathbb{K})$ (descrito no exemplo 3.1.10 (iii)) munido com a multiplicação usual de matrizes é um grupo algébrico. De fato, $Gl_n(\mathbb{K})$ é isomorfo a variedade afim $X = V(\langle x_0 \det -1\rangle) \subseteq \mathbb{A}^{n^2+1}$. A multiplicação de matrizes é uma função polinomial. Explicitamente, considere $A = (a_0, a_{11}, \ldots, a_{n-1n}, a_{nn}), B = (b_0, b_{11}, \ldots, b_{n-1n}, b_{nn}) \in X$. Se $C = m(A, B)$ então

$$c_0 = a_0 b_0 \quad e \quad c_{ij} = \sum_{1 \le k \le n} a_{ik} b_{kj}.$$

A inversa também é uma função polinomial, pois se $A = (a_0, a_{11}, \ldots, a_{n-1n}, a_{nn}) \in X$ então $i(A)$ pode ser escrita como

$$(1/\det(A), \det(A_{11})/a_0, \det(A_{21})/a_0, \ldots, \det(A_{n-1n})/a_0, \det(A_{nn})/a_0),$$

onde A_{ij} são os menores associados a A, ou seja, A_{ij} é a matriz A com a linha i e a coluna j omitidas. Em particular, a identidade de $Gl_n(\mathbb{K})$ é a matriz identidade de ordem n.

(*iv*) Seja H um subgrupo fechado de um grupo algébrico G. Então H é um grupo algébrico. Primeiro porque H é um subgrupo de G. Segundo porque, como H é fechado, H é uma variedade algébrica. Por fim, esssas estruturas de H são herdadas do grupo G e portanto a multiplicação e inversa em H são morfismos de variedades algébricas.

(*v*) Os grupos clássicos: $Sl_n(\mathbb{K})$, $O_n(\mathbb{K})$ e $Sp_{2n}(\mathbb{K})$ (descritos no exemplo 3.1.10) são grupos algébricos. De fato, $Sl_n(\mathbb{K})$, $O_n(\mathbb{K})$ são subvariedades fechadas de $Gl_n(\mathbb{K})$, enquanto $Sp_{2n}(\mathbb{K})$ é subvariedade fechada de $Gl_{2n}(\mathbb{K})$, portanto são variedades algébricas. Além disso, eles são claramente subgrupos de $Gl_n(\mathbb{K})$ e $Gl_{2n}(\mathbb{K})$ respectivamente.

(*vi*) Os subgrupos $T_n(\mathbb{K})$, $U_n(\mathbb{K})$ e $D_n(\mathbb{K})$ (descritos no exemplo 3.1.10) são algébricos, pois são subgrupos fechados de $Gl_n(\mathbb{K})$.

(*vii*) Sejam G e H dois grupos algébricos. O produto direto $G \times H$ é um grupo algébrico. A estrutura multiplicativa em $G \times H$ é a estrutura de produto direto de grupos e a estrutura de variedade algébrica em $G \times H$ é dada pela topologia de Zariski no produto de conjuntos $G \times H$. Esse é de fato o produto na categoria de grupos algébricos.

Definição 4.1.5. Seja G um grupo algébrico e V um espaço vetorial. Uma *representação racional de* G é um morfismo de grupos algébricos $\rho : G \to Gl(V)$.

Seja G um grupo algébrico. Existe uma componente irredutível do grupo G que contém o elemento identidade do grupo. A proposição a seguir afirma que essa componente é única.

Proposição 4.1.6. Se G é um grupo algébrico, então existe uma única componente irredutível de G que contém o elemento identidade.

Dem: Considere $G_1, \ldots, G_k \subseteq G$ todas as distintas componentes irredutíveis de G contendo a identidade. Como cada G_i, $i = 1, \ldots, k$, é irredutível, $G_1 \times \ldots \times G_k$ também é irredutível. Como a multiplicação é associativa e é um morfismo de grupos algébricos, $G_1 \ldots G_k \subseteq G$ é irredutível e contém a identidade. Por ser irredutível e conter a identidade de G, $G_1 \ldots G_k$ é igual a um dos G_i para algum $i = 1, \ldots, k$. Por outro lado, $G_1 \ldots G_k$ contém G_j para todo $j = 1, \ldots, k$. Consequentemente $G_j \subseteq G_i = G_1 \ldots G_k$, $\forall\ j = 1, \ldots, k$, e a única componente irredutível contendo a identidade é G_i. $\square$

Como existe uma única componente irredutível que contém a identidade, essa componente irredutível é denotada por G_0. Por ser uma componente irredutível, G_0 é fechada. A seguinte proposição compila outras propriedades de G_0.

Proposição 4.1.7. Seja G um grupo algébrico.

(*i*) G_0 é um subgrupo normal de G.

(*ii*) G_0 tem índice finito em G.

(*iii*) O conjunto de classes laterais de G_0 coincide com o conjunto de componentes irredutíveis e com o conjunto de componentes conexas de G.

(*iv*) Todo subgrupo fechado de índice finito de G contém G_0.

Dem: (*i*) Para mostrar que G_0 é subgrupo, é necessário mostrar que, para cada $g, h \in G_0$, $g^{-1} \in G_0$ e $gh \in G_0$.

Para cada $g \in G_0$, $g^{-1}.G_0$ é uma componente irredutível de G que contém e, pois $g \in G_0$ e as translações são contínuas. Portanto $g^{-1}.G_0 = G_0$. Em particular, $g^{-1} \in G_0$.

Para cada $g, h \in G_0$, hG_0 é uma componente irredutível de G que contém e. Portanto $hG_0 = G_0$. Por argumento análogo $(gh)G_0 = G_0$. Em particular, $gh \in G_0$.

Para mostrar que G_0 é normal basta mostrar que $gG_0g^{-1} = G_0$ para todo $g \in G$. Então considere $g \in G$. Por argumento análogo aos anteriores, gG_0g^{-1} é uma componente irredutível de G contendo e. Portanto $gG_0g^{-1} = G_0$.

(*ii*) As classes laterais de G_0 são imagens de G_0 por translações. Portanto toda classe lateral de G_0 é uma componente irredutível de G. Como G é noetheriano, existe uma quantidade finita de componentes irredutíveis de G. Portanto existe uma quantidade finita de classes laterais de G_0.

(*iii*) As classes laterais de G_0 são irredutíveis. Além disso, a união dessas classes laterais cobre G. Portanto elas são as componentes irredutíveis de G. Como as classes laterais de G_0 são disjuntas, elas são também as componentes conexas de G.

(*iv*) Se H for um subgrupo fechado de índice finito em G então cada uma das suas finitas classes laterais à esquerda também é fechada. Logo a união finita

$$\left(\bigcup_{g \notin H} gH \right)$$

também é fechada. Portanto seu complementar, H, é aberto. Isso significa que as classes laterais de H particionam G em união finita de abertos. Em particular, G_0 é particionado em uma união finita de abertos. Como G_0 é conexo e H contém a identidade, $G_0 \subseteq H$.

□

Pela proposição acima faz sentido definir um grupo algébrico como *conexo* quando $G = G_0$. Define-se também G_0 como *a componente conexa da identidade*.

Exemplo 4.1.8.

(*i*) Todo espaço afim é conexo. De fato, todo espaço afim é irredutível. Em particular, $G_a(\mathbb{K})$ é conexo.

(*ii*) Se um grupo algébrico G é isomorfo a um aberto principal de um espaço afim então G é conexo. De fato, um subconjunto do espaço afim é irredutível se, e somente se, seu fecho é irredutível. Em particular, $G_m(\mathbb{K})$ e $Gl_n(\mathbb{K})$ são conexos.

Para mostrar que $Sl_n(\mathbb{K})$, $T_n(\mathbb{K})$, $U_n(\mathbb{K})$ e $D_n(\mathbb{K})$ são conexos, a técnica usada será diferente.

Lema 4.1.9.

(i) Sejam U e V dois abertos densos e distintos em um grupo algébrico G. Para qualquer $g \in G$, existem $u \in U$ e $v \in V$, tais que $g = uv$, ou seja, $G = UV$.

(ii) Para todo subgrupo H de um grupo algébrico G, $\overline{H}$ é subgrupo algébrico.

(iii) Se H é um subgrupo construtível de um grupo algébrico G, então $\overline{H} = H$.

Dem: (i) Como a inversa é um isomorfismo de grupos algébricos, V^{-1} é um aberto de G. Como as translações também são isomorfismos, $g.V^{-1}$ também é um aberto de G. Como U é um aberto denso distinto de V, para todo $g \in G$, existem $u \in U$ e $v \in V$, tais que $gv^{-1} = u$.

(ii) Seja H um subgrupo de G. Como $\overline{H}$ é fechado em G, para mostrar que $\overline{H}$ é um grupo algébrico, basta mostrar que $\overline{H}$ é subgrupo de G. Como a inversa é isomorfismo do grupo algébrico G, $\overline{H}$ é fechado pela inversa. De fato, $(\overline{H})^{-1} = \overline{H^{-1}} = \overline{H}$. Agora basta mostrar que $\overline{H}$ é fechado pela multiplicação. Como as translações são isomorfismos de G, $h\overline{H} = \overline{hH} = \overline{H}$, para todo $h \in H$. Portanto $H\overline{H} \subseteq \overline{H}$. Usando o fato anterior e o fato das translações serem isomorfismos, $\overline{Hg} = \overline{H}g \subseteq \overline{H}$ para todo $g \in \overline{H}$. Portanto $\overline{H}$ é um subgrupo algébrico.

(iii) Como H é construtível, existe um aberto denso $U \subseteq H$ que também é aberto denso em $\overline{H}$. Usando os dois itens anteriores, $\overline{H} = UU$. Como $UU \subseteq HH = H$, $\overline{H} \subseteq H$. Portanto H é fechado.

□

As seguintes propriedades são básicas para lidar com grupos algébricos e morfismos entre eles.

Proposição 4.1.10. Seja $\varphi : G \to H$ um morfismo entre grupos algébricos.

(i) $\ker(\varphi) \subseteq G$ e $im(\varphi) \subseteq H$ são subgrupos algébricos fechados.

(ii) A imagem da componente conexa da identidade de G é a componente conexa da identidade da imagem de G, ou seja, $\varphi(G_0) = \varphi(G)_0$.

(iii) Teorema do núcleo-imagem: $\dim(G) = \dim(\ker(\varphi)) + \dim(im(\varphi))$.

Dem: (i) $\ker(\varphi)$ é imagem inversa de um ponto, a saber $\ker(\varphi) = \varphi^{-1}(e_H)$. Como φ é contínua, $\ker(\varphi)$ é fechado em G. A imagem, por sua vez, é um subgrupo de H. De fato, $im(\varphi)$ é imagem de G, portanto é construtível. Usando esse fato e o item (iii) da proposição 4.1.9, $im(\varphi)$ é fechada.

(ii) G_0 é um subgrupo normal, fechado e conexo de G. Como φ é contínua, $\varphi(G_0)$ é conexo. Pelo item (i), $\varphi(G_0)$ é um subgrupo fechado de $im(\varphi)$. Como φ é homomorfismo de grupos, $\varphi(g)(\varphi(G_0)) = \varphi(gG_0)$, ou seja, a imagem das classes laterais de G_0 são as classes laterais da imagem de G_0. Como G_0 tem índice finito em G, $\varphi(G_0)$ tem índice finito em $im(\varphi)$. Usando o item (iv) da proprosição 4.1.7 e o fato de que $\varphi(G_0)$ é um subgrupo fechado e conexo de índice finito em $im(\varphi)$, conclui-se que $\varphi(G_0) = \varphi(G)_0$.

(*iii*) Usando o teorema 4.3 do livro [Hum2], $\dim(G) - \dim(\varphi(G)) = \dim(\varphi^{-1}(g))$ para algum $g \in \varphi(G)$. Como as fibras são isomorfas ao núcleo, conclui-se que: $\dim(G) - \dim(\varphi(G)) = \dim(\ker(\varphi))$.

$\square$

Proposição 4.1.11. Se um subgrupo H de um grupo algébrico G é gerado (como grupo) por uma família de subgrupos fechados e conexos de G, então H é um grupo algébrico conexo.

Essa proposição é corolário do seguinte teorema:

Teorema 4.1.12. Sejam G um grupo algébrico, $(X_i)_{i\in I}$ uma família de variedades irredutíveis e $\varphi_i : X_i \to G$ uma família de morfismos, tais que $\varphi_i(X_i) = Y_i \subseteq G$ contêm a identidade de G, $\forall\ i \in I$. Seja ainda C a intersecção de todos os subgrupos fechados que contêm $\bigcup_i Y_i$. Então:

(*i*) C é conexo;

(*ii*) Existem um subconjunto finito de índices $\{i_1, \ldots, i_k\} \subset I$ e números $e_1, \ldots, e_k$, com $e_j = \pm 1$ (para todo $j = 1, \ldots, k$), tal que $C = Y_{i_1}^{e_1} \ldots Y_{i_k}^{e_k}$, onde $Y_{i_j}^{-1} = \{x^{-1} \in G \mid x \in Y_{i_j}\}$, $j = 1, \ldots, k$.

Dem: (*i*) Sem perda de generalidade, suponha que os morfismos : $x \mapsto \varphi_i(x)^{-1}$ também estejam na família $(\varphi_i)_{i\in I}$. Para cada sequência finita de índices $i = (i_1, \ldots, i_k) \in I^k$, denote $Y_i = Y_{i_1} \ldots Y_{i_k}$. Como Y_i é imagem da variedade $X_{i_1} \times \ldots \times X_{i_k}$ pelo morfismo $m \circ (\varphi_{i_1} \times \ldots \times \varphi_{i_k})$, onde m denota a multiplicação de G, então Y_i é construtível e $\overline{Y_i}$ é uma variedade irredutível contendo e, $\forall\ i \in I^k$. Agora, usando a condição de maximalidade da componente irredutível G_0, é possível achar uma sequência $i \in I$ para a qual $\overline{Y_i}$ é maximal.

Dados $i, j \in I$, $\overline{Y_i Y_j} \subseteq \overline{Y}_{(i,j)}$, onde (i, j) é a sequência em $i = (i_1, \ldots, i_l) \in I^l$ obtida por justaposição de i e j. De fato, para todo $y \in Y_j$ a função : $x \mapsto xy$ é uma função de Y_i em $Y_{(i,j)}$ e consequentemente de $\overline{Y_i}$ em $\overline{Y}_{(i,j)}$. Analogamente, para cada $x \in Y_i$.

Como $\overline{Y_i}$ é maximal e $e \in \overline{Y_j}$ para todo $j \in I$, então: $\overline{Y_i} \subseteq \overline{Y_i Y_j} \subseteq \overline{Y}_{(i,j)} = \overline{Y_i}$. Tomando $i = j$, obtem-se que $\overline{Y_i}$ é fechado sob multiplicação. Tomando $j \in I$, tal que $Y_j = Y_i^{-1}$, obtem-se que $\overline{Y_i}$ é fechado sob inversa. Portanto $\overline{Y_i}$ é um subgrupo fechado de G.

(*ii*) Y_i é construtível. Usando o lemma 4.1.9, obtem-se que $\overline{Y_i} = Y_i.Y_i = Y_{(i,i)}$. A sequência (i, i) satisfaz (*ii*).

$\square$

Exemplo 4.1.13. Considere a seguinte notação. Para cada $n \in \mathbb{N}$ e para cada $i, j = 1, \ldots, n$, as matrizes e_{ij} denotam as matrizes de ordem n com todas as entradas nulas exceto na posição (ij), onde a entrada é 1. Para cada $i, j \in \{1, \ldots, n\}$, considere G_{ij} como o subgrupo algébrico de $Gl_n(\mathbb{K})$ gerado por $(id_n + ke_{ij})$, $k \in \mathbb{K}$. Para todo $i, j, \in \mathbb{N}$, G_{ij} é isomorfo a $G_a(\mathbb{K})$, portanto G_{ij} é conexo. Usando o resultado acima:

(*i*) $Sl_n(\mathbb{K})$ é conexo pois é gerado por $\{G_{ij} \mid 1 \leq i \neq j \leq n\}$.

(*ii*) $T_n(\mathbb{K})$ é conexo pois é gerado por $\{G_{ij} \mid i \leq j\}$.

(iii) $U_n(\mathbb{K})$ é conexo pois é gerado por $\{G_{ij} \mid i < j\}$.

(iv) $D_n(\mathbb{K})$ é conexo pois é gerado por $\{G_{ii} \mid i = 1, \ldots, n\}$.

A seguinte definição será útil, quando considerarmos grupos de Chevalley.

Definição 4.1.14. Um grupo algébrico G é chamado de *semissimples* quando não contém nenhum subgrupo fechado, conexo, comutativo e normal diferente de $\{e\}$.

No contexo de grupos de Lie também é comum definir grupo simplesmente conexo. Os grupos de Lie simplesmente conexos são caracterizados pelo fato de que todo recobrimento é trivial. No contexto de grupos algébricos, existe uma definição análoga porém mais técnica.

Definição 4.1.15. Sejam G, G' grupos algébricos conexos. Um morfismo de grupos algébricos $\varphi : G' \to G$ é uma *isogenia* quando φ é sobrejetora e tem núcleo finito. O grupo G é *simplesmente conexo* quando não admite nenhuma isogenia não trivial $\varphi : \widetilde{G} \to G$ de um grupo algébrico conexo $\widetilde{G}$.

Para mais detalhes, vide [Tak1].

No capítulo anterior, definimos variedades afins do ponto de vista clássico e em seguida do ponto de vista funtorial, como um R-funtor. Como os grupos algébricos também são variedades afins, vamos definí-los do ponto de vista funtorial também. Considere toda álgebra como sendo uma álgebra comutativa com identidade.

Definição 4.1.16. Seja R um anel. Defina um *R-funtor de grupo* como um funtor da categoria de R-álgebras para a categoria de grupos.

Observe que todo funtor de grupo corresponde a um R-funtor. De fato, considere $G : \mathbf{Alg}_R \to \mathbf{Grp}$ um funtor de grupo. Compondo G com o funtor de esquecimento $E : \mathbf{Grp} \to \mathbf{Sets}$, obtemos um R-funtor.

Definição 4.1.17. Sejam R um anel e G um R-funtor de grupo. Um subfuntor $H \subseteq G$ é um *subfuntor de grupo* quando $H(A)$ é um subgrupo de $G(A)$ para todo $A \in \mathbf{Alg}_R$. Um subfuntor de grupo $H \subseteq G$ é chamado de *normal* quando $H(A)$ é subgrupo normal de $G(A)$ para todo $A \in \mathbf{Alg}_R$.

Seja G' um R-funtor de grupo. Defina o conjunto de *morfismos de R-funtores de grupos*, $Mor(G, G')$, como o conjunto de morfismos (transformações naturais) de G para G' vistos como R-funtores. Defina o conjunto de *homomorfismos de R-funtores de grupos*, $Hom(G, G')$, como o conjunto de morfismos (transformações naturais) de G para G' vistos como R-funtores de grupos. Ou seja, os elementos de $Hom(G, G')$ são os elementos $\eta \in Mor(G, G')$, tais que $\eta(A) : G(A) \to G'(A)$ são homomorfismos de grupos para todo $A \in \mathbf{Alg}_R$.

Proposição 4.1.18. Sejam R um anel e G um R-funtor de grupo.

(i) A intersecção de subfuntores de grupo de G é um subfuntor de grupo de G.

(ii) Sejam G' um R-funtor de grupo e $H' \subseteq G'$ um subfuntor de grupo de G'. Se $\varphi \in Hom(G, G')$, então $\varphi^{-1}(H')$ é um subfuntor de grupo de G.

(iii) Se G' é um R-funtor de grupo, então o produto $G \times G'$ é um R-funtor de grupo.

Definição 4.1.19. Seja R um anel. Um *R-esquema de grupo* é concomitantemente um R-funtor de grupo e um esquema afim. Um esquema de grupo é chamado de *algébrico* ou de *reduzido* quando, visto como esquema afim, for, respectivamente, algébrico ou reduzido.

Exemplo 4.1.20. Seja $\mathbb{K}$ um corpo.

(i) Os funtores da forma $Hom_{Alg_{\mathbb{K}}}(\mathbb{K}[G], \cdot)$, onde G é um grupo algébrico linear, são esquemas de grupo.

(ii) O funtor $Hom_{Alg_{\mathbb{K}}}(\mathbb{K}[x], \cdot)$ é um esquema de grupo. Esse esquema é chamado de *Grupo aditivo de* $\mathbb{K}$ e denotado por $G_a(\mathbb{K})$.

(iii) O funtor $Hom_{Alg_{\mathbb{K}}}(\mathbb{K}[x, x^{-1}], \cdot)$ é um esquema de grupo. Esse esquema é chamado de *Grupo multiplicativo de* $\mathbb{K}$ e denotado por $G_m(\mathbb{K})$.

(iv) O funtor $Hom_{Alg_{\mathbb{K}}}(\mathbb{K}[Sl_n], \cdot)$ é um esquema de grupo. Esse esquema é chamado de *Grupo especial linear de* $\mathbb{K}$ e denotado por $Sl_n(\mathbb{K})$.

Sejam G um grupo algébrico sobre $\mathbb{K}$ e $\mathbb{K}[G]$ sua álgebra de funções regulares. Considere o esquema de grupo $\mathcal{G} = Sp_{\mathbb{K}}\mathbb{K}[G]$. Tal construção associa a cada grupo algébrico um esquema de grupo algébrico e reduzido. Por outro lado, é possível reconstruir G a partir de $\mathcal{G}$.

4.2 Álgebras de Lie de grupos algébricos

Na teoria de grupos de Lie é usual associar a cada grupo de Lie G uma álgebra de Lie. Essa álgebra de Lie é definida de duas formas: como o espaço tangente a identidade da variedade G ou como a álgebra dos campos invariantes à esquerda no fibrado tangente de G. A ideia dessa seção é fazer definições análogas para grupos algébricos.

Considere $\mathbb{K}$ um corpo algebricamente fechado e a partir deste ponto, álgebras significarão álgebras associativas, não necessariamente comutativas e não necessariamente com unidade.

Definição 4.2.1. Seja G um grupo algébrico. Defina $\mathfrak{g}$, a *álgebra de Lie* de G, como o espaço tangente a variedade G na identidade do grupo.

Como $(\mathfrak{m}_e/\mathfrak{m}_e{}^2)^*$ é um espaço vetorial sobre o corpo $\mathcal{O}_e/\mathfrak{m}_e$, T_eG admite uma estrutura de espaço vetorial. Além disso, o conjunto dos funcionais lineares $Hom((\mathfrak{m}_e/\mathfrak{m}_e{}^2), (\mathcal{O}_e/\mathfrak{m}_e))$ tem estrutura de álgebra. De fato, como a multiplicação $m : G \times G \to G$ é um morfismo de grupos algébricos, faz sentido considerar o seu comorfismo $m^* : \mathbb{K}[G] \to \mathbb{K}[G] \otimes \mathbb{K}[G]$. Agora considere a multiplicação em T_eG induzida por esse comorfismo:

$$\mathsf{x}.\mathsf{y} = (\mathsf{x} \otimes \mathsf{y}) \circ m^*, \quad \forall\, \mathsf{x}, \mathsf{y} \in T_eG.$$

Usando a estrutura de álgebra, é possível munir T_eG de uma estrutura de álgebra de Lie com o comutador. Explicitamente, o colchete é:

$$\begin{aligned}[\mathsf{x}, \mathsf{y}](f) &= (\mathsf{x}.\mathsf{y} - \mathsf{y}.\mathsf{x})(f) \\ &= (\mathsf{x} \otimes \mathsf{y}) \circ m^*(f) - (\mathsf{y} \otimes \mathsf{x}) \circ m^*(f),\end{aligned}$$

para cada $\mathsf{x}, \mathsf{y} \in T_eG,\ f \in \mathbb{K}[G]$.

Seja $\varphi : G \to H$ um morfismo entre dois grupos algébricos. Como descrito na seção 3.3, existe um morfismo entre as álgebras de Lie correspondentes, a saber, $d_e\varphi : \mathfrak{g} \to \mathfrak{h}$, onde $d_e\varphi(\mathsf{x}) = \mathsf{x} \circ \varphi^*$ para cada $\mathsf{x} \in \mathfrak{g}$.

Seja H um subgrupo fechado de um grupo algébrico G. A inclusão $\varphi : H \hookrightarrow G$ é um morfismo injetor de variedades algébricas. Portanto φ pode ser visto como um isomorfismo entre H e um subgrupo fechado de G. Dessa forma, a derivada de φ é uma inclusão de álgebras de Lie $d_e\varphi : \mathfrak{h} \hookrightarrow \mathfrak{g}$. Consequentemente $\mathfrak{h}$ é uma subálgebra de $\mathfrak{g}$. Além disso, o comorfismo

$$\varphi^* : \mathbb{K}[G] \to \mathbb{K}[H] \xrightarrow{\simeq} \mathbb{K}[G]/I(H)$$

é sobrejetor.

Como todo grupo algébrico G é suave, a identidade de G é sempre um ponto regular. Portanto a dimensão da álgebra de Lie de G é igual a dimensão de G.

Exemplo 4.2.2. Vários exemplos de álgebras de Lie já foram calculados no capítulo anterior.

(i) Para cada $n \in \mathbb{N}$, $T_0(\mathbb{A}^n) \simeq \mathbb{A}^n$. Em particular, $T_e(G_a(\mathbb{K})) \simeq G_a(\mathbb{K}) \simeq \mathbb{A}^1$, munido do colchete trivial.

(ii) $T_e(G_m(\mathbb{K})) \simeq \mathbb{A}^1$, munido do colchete trivial.

(iii) Para cada $n \in \mathbb{N}$, $T_e(Gl_n(\mathbb{K})) \simeq \mathfrak{gl}_n$.

(iv) Para cada $n \in \mathbb{N}$, $T_e(Sl_n(\mathbb{K})) \simeq \mathfrak{sl}_n$.

(v) Para cada $n \in \mathbb{N}$, $T_e(T_n(\mathbb{K})) \simeq \mathfrak{t}_n$.

(vi) Para cada $k \in \mathbb{N}$, $T_e(U_k(\mathbb{K})) \simeq \mathfrak{n}_k$.

(vii) Para cada $n \in \mathbb{N}$, $T_e(D_n(\mathbb{K})) \simeq \mathfrak{d}_n$.

Quando se tem um grupo de Lie, define-se uma estrutura de álgebra de Lie no espaço vetorial de campos invariantes à esquerda no fibrado tangente da variedade. Usando essa ideia é possível caracterizar a álgebra de Lie de grupos algébricos de forma análoga.

Seja G um grupo algébrico. Para cada $g \in G$, considere as funções ${D_g}^*, {E_g}^* : \mathbb{K}[G] \to \mathbb{K}[G]$ definidas por ${D_g}^*(f) = f \circ D_g$ e ${E_g}^*(f) = f \circ E_{g^{-1}}$, $\forall\ f \in \mathbb{K}[G]$.

Definição 4.2.3. Considere G um grupo algébrico sobre o corpo $\mathbb{K}$. Defina $\mathcal{L}(G)$ como o conjunto de derivações do anel de funções regulares de G que são invariantes por translações à esquerda, ou seja, $\mathcal{L}(G) = \{\delta \in Der(\mathbb{K}[G]) \mid {E_g}^* \circ \delta = \delta \circ {E_g}^*,\ \forall\ g \in G\}$.

Proposição 4.2.4. Seja G um grupo algébrico. $\mathcal{L}(G)$ tem estrutura de álgebra de Lie.

Dem: As derivações formam uma álgebra de Lie, munidas do colchete definido pelo comutador de duas derivações. De fato, se $d_1, d_2 \in Der(\mathbb{K}[G])$ então, para quaisquer $f, g \in \mathbb{K}[G]$, tem-se

$$\begin{aligned} d_1 \circ d_2(fg) &= d_1(fd_2(g) + d_2(f)g) \\ &= d_1(fd_2(g)) + d_1(d_2(f)g) \\ &= fd_1 \circ d_2(g) + d_1(f)d_2(g) + d_1 \circ d_2(f)g + d_2(f)d_1(g) \end{aligned}$$

$$
\begin{aligned}
d_2 \circ d_1(fg) &= d_2(fd_1(g) + d_1(f)g) \\
&= d_2(fd_1(g)) + d_2(d_1(f)g) \\
&= fd_2 \circ d_1(g) + d_2(f)d_1(g) + d_2 \circ d_1(f)g + d_1(f)d_2(g).
\end{aligned}
$$

Portanto $(d_1 \circ d_2 - d_2 \circ d_1)(fg) = (d_1 \circ d_2 - d_2 \circ d_1)(f)g + f(d_1 \circ d_2 - d_2 \circ d_1)(g)$.

As derivações invariantes por translações à esquerda formam uma subálgebra de Lie de $Der(\mathbb{K}[G])$. De fato, se $d_1, d_2 \in \mathcal{L}(G)$, então

$$
\begin{aligned}
{E_g}^* \circ [d_1, d_2] &= {E_g}^* \circ d_1 \circ d_2 - {E_g}^* \circ d_2 \circ d_1 \\
&= d_1 \circ {E_g}^* \circ d_2 - d_2 \circ {E_g}^* \circ d_1 \\
&= d_1 \circ d_2 \circ {E_g}^* - d_2 \circ d_1 \circ {E_g}^* \\
&= [d_1, d_2] \circ {E_g}^*.
\end{aligned}
$$

Portanto $\mathcal{L}(G)$ munido do colchete definido pelo comutador de derivações tem estrutura de álgebra de Lie. $\square$

Observe que, como as derivações de $\delta \in \mathcal{L}(G)$ são invariantes à esquerda e E_g age transitivamente em G, para toda $f \in \mathbb{K}[G]$, a avaliação de $\delta(f)$ em qualquer ponto do grupo G determina unicamente a avaliação de $\delta(f)$ em todo ponto de G. De fato,

$$
\begin{aligned}
\delta f(g) &= \delta f(E_g(e)) \\
&= \delta f \circ E_g(e) \\
&= E^*_{g^{-1}}(\delta f)(e) \\
&= \delta(E^*_{g^{-1}} f)(e).
\end{aligned}
$$

Consequentemente para se conhecer a derivação basta conhecer a imagem da derivação avaliada no elemento identidade do grupo G.

Por isso considere a função $\delta_e : \mathbb{K}[G] \to \mathbb{K}$, que a cada função regular, $f \in \mathbb{K}[G]$ associa $\delta_e(f) = \delta f(e)$. Dadas duas funções regulares $f_1, f_2 \in \mathbb{K}[G]$, $\delta_e(f_1 f_2) = \delta(f_1 f_2)(e)$. Como δ é uma derivação de $\mathbb{K}[G]$,

$$
\begin{aligned}
\delta(f_1 f_2)(e) &= \delta(f_1)(e) f_2(e) + f_1(e)\delta(f_2)(e) \\
&= \delta_e(f_1) f_2(e) + f_1(e)\delta_e(f_2).
\end{aligned}
$$

Isso significa que $\delta_e(f_1 f_2) = \delta_e(f_1) f_2(e) + f_1(e)\delta_e(f_2)$, ou seja, $\delta_e \in T_e G$.

Lembrando que os elementos de $(\mathfrak{m}_e/{\mathfrak{m}_e}^2)^*$ também só dependem do valor da função regular em torno do elemento identidade, para cada $\mathsf{x} \in T_e G$, defina a *convolução à direita* por x como uma função $*\mathsf{x}$, que, para cada $f \in \mathbb{K}[G]$ e $g \in G$, associa $f * \mathsf{x}(g) = \mathsf{x}(E^*_{g^{-1}} f)$.

Considere duas funções regulares $f_1, f_2 \in \mathbb{K}[G]$ e um elemento da álgebra de Lie, $\mathsf{x} \in T_e G$. Para cada $g \in G$,

$$
\begin{aligned}
(f_1 f_2) * \mathsf{x}(g) &= \mathsf{x}(E^*_{g^{-1}}(f_1 f_2)) \\
&= \mathsf{x}(E^*_{g^{-1}}(f_1) E^*_{g^{-1}}(f_2)) \\
&= E^*_{g^{-1}} f_1(e).\mathsf{x}(E^*_{g^{-1}} f_2) + \mathsf{x}(E^*_{g^{-1}} f_1).E^*_{g^{-1}} f_2(e) \\
&= f_1(g).(f_2 * \mathsf{x}(g)) + (f_1 * \mathsf{x}(g)).f_2(g).
\end{aligned}
$$

Isso significa que $(f_1 f_2) * \mathsf{x} = f_1(f_2 * \mathsf{x}) + (f_1 * \mathsf{x}) f_2$, ou seja, $*\mathsf{x} \in \mathcal{L}(G)$.

Considere, por um lado, a função $\varphi_e : \mathcal{L}(G) \to T_e G$, que a cada $\delta \in \mathcal{L}(G)$ associa $\varphi_e(\delta) = \delta_e$, ou seja, a avaliação da derivação na identidade do grupo G. Por outro lado, considere a função convolução $* : T_e G \to \mathcal{L}(G)$, que a cada $\mathsf{x} \in T_e G$ associa $*\mathsf{x} \in \mathcal{L}(G)$. Pela construção feita acima, essas duas funções são inversas uma da outra.

Essas observações demonstram o teorema a seguir.

Teorema 4.2.5. Sejam G um grupo algébrico e $\mathfrak{g} = T_e G$ seu espaço tangente na identidade. A função φ_e é um isomorfismo de álgebras de Lie entre $\mathcal{L}(G)$ e $\mathfrak{g}$.

O isomorfismo acima permite transitar livremente entre essas duas caracterizações da álgebra de Lie de um grupo algébrico. Ou seja, ela permite ver a álgebra de Lie de um grupo algébrico G como o espaço vetorial $(\mathfrak{m}_e/\mathfrak{m}_e{}^2)^*$ ou como um conjunto de funções agindo no anel de funções regulares $\mathbb{K}[G]$. Os dois pontos de vista serão úteis.

Proposição 4.2.6. Sobre um corpo de característica zero, um grupo algébrico conexo é semissimples se, e somente se, sua álgebra de Lie é semissimples.

Dem: [Hum2], p.89. $\square$

4.3 Álgebras de Hopf associadas a grupos algébricos

Nesta seção, algumas álgebras de Hopf associadas a grupos algébricos serão descritas.

Considere um grupo algébrico G. Usando o isomorfismo entre $T_e G$ e $\mathcal{L}(G)$ descrito no teorema 4.2.5, é possível identificar a álgebra universal envelopante da álgebra de Lie de G com uma álgebra de funções agindo no anel de funções regulares de G. Como visto no capítulo 1, a álgebra universal envelopante de uma álgebra de Lie é uma álgebra de Hopf.

Além da álgebra universal envelopante da álgebra de Lie de um grupo algébrico, a álgebra de funções regulares e a álgebra de distribuições de um grupo algébrico também têm estrutura de álgebra de Hopf.

Considere $\mathbb{K}$ um corpo algebricamente fechado.

4.3.1 Álgebra de funções regulares

Seja G um grupo algébrico sobre $\mathbb{K}$. Denote por $m : G \times G \to G$ a multiplicação do grupo, por $e \in G$ seu elemento identidade e por $i : G \to G$ a sua inversa. A álgebra de funções regulares $\mathbb{K}[G]$ pode ser munida de uma estrutura de álgebra de Hopf.

A multiplicação e a unidade de $\mathbb{K}[G]$ foram descritas na seção 3.1.2.

A comultiplicação é dada pelo comorfismo de m, $\Delta = m^* : \mathbb{K}[G] \to \mathbb{K}[G] \otimes \mathbb{K}[G]$. Explicitamente, para todo $\varphi \in \mathbb{K}[G]$, $\Delta(\varphi)(g, h) = \varphi \circ m(g, h) = \varphi(gh)$. A comultiplicação é coassociativa. De fato, para todo $\varphi \in \mathbb{K}[G]$,

$$\begin{aligned}
((\Delta \otimes id) \circ \Delta)(\varphi)(a,b,c) &= ((\Delta \otimes id)(\varphi \circ m))(a,b,c) \\
&= (\varphi \circ m \circ (m \otimes id))(a,b,c) \\
&= \varphi((ab)c) \\
&e \\
((id \otimes \Delta) \circ \Delta(\varphi))(a,b,c) &= ((id \otimes \Delta)(\varphi \circ m))(a,b,c) \\
&= (\varphi \circ m \circ (id \otimes m))(a,b,c) \\
&= \varphi(a(bc)),
\end{aligned}$$

para quaisquer $a, b, c \in G$. Como a multiplicação do grupo é associativa, $(\Delta \otimes id) \circ \Delta = (id \otimes \Delta) \circ \Delta$.

A counidade, $\varepsilon : \mathbb{K}[G] \to \mathbb{K}$, é tal que, para cada $\varphi \in \mathbb{K}[G]$, $\varepsilon(\varphi) = \varphi(e)$. Para quaisquer $\varphi \in \mathbb{K}[G]$ e $g \in G$,

$$\begin{aligned}
((id \otimes \varepsilon) \circ \Delta(\varphi))(g) &= ((id \otimes \varepsilon) \circ (\varphi \circ m))(g) \\
&= \left((id \otimes \varepsilon)\left(\sum_i \varphi_i \otimes \psi_i\right)\right)(g) \\
&= \left(\sum_i \varphi_i \psi_i(e)\right)(g) \\
&= \sum_i \varphi_i(g)\psi_i(e) \\
&= (\Delta(\varphi))(g,e) \\
&= (\varphi \circ m)(g,e) \\
&= \varphi(g),
\end{aligned}$$

$$\begin{aligned}
((\varepsilon \otimes id) \circ \Delta(\varphi))(g) &= ((\varepsilon \otimes id) \circ (\varphi \circ m))(g) \\
&= \left((\varepsilon \otimes id)\left(\sum_i \varphi_i \otimes \psi_i\right)\right)(g) \\
&= \left(\sum_i \varphi_i(e)\psi_i\right)(g) \\
&= \sum_i \varphi_i(e)\psi_i(g) \\
&= (\Delta(\varphi))(e,g) \\
&= (\varphi \circ m)(e,g) \\
&= \varphi(g).
\end{aligned}$$

Isso mostra que os diagramas de counidade (1.3.4) são comutativos.

Para completar a estrutura de álgebra de Hopf, a antípoda é dada pelo comorfismo de i, $S = i^* : \mathbb{K}[G] \to \mathbb{K}[G]$. Explicitamente, $S(\varphi)(g) = \varphi(g^{-1})$, para cada $\varphi \in \mathbb{K}[G]$ e $g \in G$.

Para cada $\varphi \in \mathbb{K}[G]$ e $g \in G$,

$$\begin{aligned}((u \circ \varepsilon)(\varphi))(g) &= u(\varphi(e))g \\ &= \varphi(e),\end{aligned}$$

$$\begin{aligned}
((\mu \circ (S \otimes id) \circ \Delta)(\varphi))(g) &= (\mu \circ (S \otimes id) \circ (\varphi \circ m))(g) \\
&= \left(\mu \circ (S \otimes id)\left(\sum_i \varphi_i \otimes \psi_i\right)\right)(g) \\
&= \mu\left(\sum_i S(\varphi_i) \otimes \psi_i\right)(g) \\
&= \left(\sum_i S(\varphi_i)\psi_i\right)(g) \\
&= \sum_i \varphi_i(g^{-1})\psi_i(g) \\
&= \Delta(\varphi)(g^{-1}, g) \\
&= (\varphi \circ m)(g^{-1}, g) \\
&= \varphi(e),
\end{aligned}$$

$$\begin{aligned}
((\mu \circ (id \otimes S) \circ \Delta)(\varphi))(g) &= (\mu \circ (id \otimes S) \circ (\varphi \circ m))(g) \\
&= \left(\mu \circ (id \otimes S)\left(\sum_i \varphi_i \otimes \psi_i\right)\right)(g) \\
&= \mu\left(\sum_i \varphi_i \otimes S(\psi_i)\right)(g) \\
&= \left(\sum_i \varphi_i S(\psi_i)\right)(g) \\
&= \sum_i \varphi_i(g)\psi_i(g^{-1}) \\
&= \Delta(\varphi)(g, g^{-1}) \\
&= (\varphi \circ m)(g, g^{-1}) \\
&= \varphi(e).
\end{aligned}$$

Isso mostra que $\mu \circ (S \otimes id) \circ \Delta = u \circ \varepsilon = \mu \circ (id \otimes S) \circ \Delta$, ou seja, os diagramas (1.3.4) da aplicação antípoda são comutativos.

Exemplo 4.3.1. Considere o grupo aditivo $G_a(\mathbb{K})$ (4.1.4 (i)) isomorfo a $\mathbb{A}^1$. Como descrito no exemplo 3.1.20, a álgebra afim $\mathbb{K}[\mathbb{A}^1]$ é isomorfa a álgebra de polinômios $\mathbb{K}[x]$. A multiplicação da álgebra de Hopf $\mathbb{K}[G_a]$ é a multiplicação usual da álgebra de polinômios, a saber

$$\mu(x^i, x^j) = x^{i+j}, \quad \forall\ i, j \in \mathbb{N}.$$

A unidade é o morfismo injetor de anéis $u : \mathbb{K} \to \mathbb{K}[x]$,

$$u(k) = kx^0, \quad \forall\ k \in \mathbb{K}.$$

A comultiplicação é por um lado,

$$\Delta(x^k)(a,b) = \sum_{0 \leq i,j} c_{ij} x^i(a) x^j(b) = \sum_{0 \leq i,j} c_{ij} a^i b^j,$$

para alguns $c_{ij} \in \mathbb{K}$, e por outro lado,

$$\Delta(x^k)(a,b) = x^k \circ m(a,b) = (a+b)^k = \sum_{l=0}^{k} \binom{k}{l} a^l b^{k-l},$$

para todo $a, b \in G_a$. Isso faz com que $c_{ij} = \delta_{i,l}\delta_{j,k-l}\binom{k}{l}$, $\forall\ i,j \geq 0$. Portanto:

$$\Delta(1) = 1 \otimes 1, \quad \Delta(x^k) = (x \otimes 1 + 1 \otimes x)^k, \quad \forall\ k \in \mathbb{N}^\bullet.$$

A counidade é dada por

$$\varepsilon(1) = 1(0) = 1 \quad e \quad \varepsilon(x^k) = x^k(0) = 0, \quad \forall\ k \in \mathbb{N}^\bullet.$$

A antípoda, por sua vez, é dada por $S(x^k) = x^k \circ i$, $\forall\ k \in \mathbb{N}$. Para cada $g \in G_a$, $(x^k \circ i)(g) = x^k(-g) = (-g)^k$. Portanto,

$$S(x^k) = (-x)^k, \quad \forall\ k \in \mathbb{N}.$$

Exemplo 4.3.2. Considere o grupo multiplicativo $G_m(\mathbb{K})$ (4.1.4 (*ii*)) isomorfo a $\mathbb{A}^{1^\bullet}$. Como descrito no exemplo 3.1.20, a álgebra afim $\mathbb{K}[\mathbb{A}^{1^\bullet}]$ é isomorfa a álgebra de polinômios de Laurent em uma variável, $\mathbb{K}[t, t^{-1}]$. A multiplicação da álgebra de Hopf é a multiplicação usual da álgebra associativa $\mathbb{K}[t, t^{-1}]$, a saber,

$$\mu(t^i, t^j) = t^{i+j}, \quad \forall\ i,j \in \mathbb{Z}.$$

A unidade é dada por

$$u(k) = kt^0, \quad \forall\ k \in \mathbb{K}.$$

A comultiplicação é, por um lado,

$$\Delta(t^k)(a \otimes b) = \sum_{i,j \in \mathbb{Z}} c_{ij} t^i(a) t^j(b) = \sum_{i,j \in \mathbb{Z}} c_{ij} a^i b^j,$$

para alguns $c_{ij} \in \mathbb{K}$, e por outro lado,

$$\Delta(t^k)(a \otimes b) = (t^k \circ m)(a \otimes b) = (ab)^k = a^k b^k,$$

para todo $a \otimes b \in G_m \otimes G_m$. Isso faz com que $c_{ij} = \delta_{i,k}\delta_{j,k}\ \forall\ i,j \in \mathbb{Z}$. Portanto:

$$\Delta(t^k) = t^k \otimes t^k, \quad \forall\ k \in \mathbb{Z}.$$

A counidade é dada por

$$\varepsilon(t^k) = t^k(1) = 1, \quad \forall\ k \in \mathbb{Z}.$$

A antípoda, por sua vez, é dada por $S(t^k) = t^k \circ i\ \forall\ k \in \mathbb{Z}$. Para cada $g \in G_m$, $(t^k \circ i)(g) = t^k(g^{-1}) = g^{-k}$. Portanto,

$$S\left(t^k\right) = t^{-k}, \quad \forall\ k \in \mathbb{Z}.$$

Exemplo 4.3.3. Considere o grupo linear especial $Sl_2(\mathbb{K})$. Como descrito no exemplo 3.1.20, a álgebra afim $\mathbb{K}[Sl_2]$ é isomorfa a $\frac{\mathbb{K}[x_{11},x_{12},x_{21},x_{22}]}{\langle x_{11}x_{22}-x_{21}x_{12}-1\rangle}$. A multiplicação da álgebra de Hopf é a multiplicação usual da álgebra associativa de polinômios. A unidade é dada pelo morfismo injetor de anéis $u : \mathbb{K} \to \mathbb{K}[Sl_2]$.

A comultiplicação é, por um lado,

$$\Delta(x_{ij})(a,b) = \sum_{k,l,m,n,s,t} c(k,l,m,n,s,t)x_{kl}^t(a)x_{mn}^s(b) = \sum_{k,l,m,n,s,t} c(k,l,m,n,s,t)a_{kl}^t b_{mn}^s,$$

para alguns $c(k,l,m,n,s,t) \in \mathbb{K}$, e por outro lado,

$$\Delta(x_{ij})(a,b) = (x_{ij} \circ m)(a,b) = a_{i1}b_{1j} + a_{i2}b_{2j},$$

para todo $a, b \in Sl_2(\mathbb{K})$, $i,j \in \{1,2\}$. Isso faz com que $c(k,l,m,n,s,t) = \delta_{t,1}\delta_{s,1}\delta_{k,i}\delta_{l,m}\delta_{n,j}$. Portanto:

$$\Delta(x_{ij}^n) = \big(x_{i1}x_{1j} + x_{i2}x_{2j}\big)^n, \quad \forall\, n \in \mathbb{N}, i,j \in \{1,2\}.$$

A counidade é dada por

$$\varepsilon(x_{ij}) = x_{ij}(id_2) = \delta_{i,j}, \quad \forall\, i,j \in \{1,2\}.$$

A antípoda, por sua vez, é dada por $S(x_{ij}) = x_{ij} \circ i$. Então

$$S(x_{11}^{k_{11}}x_{12}^{k_{12}}x_{21}^{k_{21}}x_{22}^{k_{22}}) = (-1)^{k_{12}+k_{21}}x_{11}^{k_{22}}x_{12}^{k_{12}}x_{21}^{k_{21}}x_{22}^{k_{11}}, \quad \forall\, k_{11}, k_{12}, k_{21}, k_{22} \in \mathbb{N}.$$

Proposição 4.3.4. Sejam G um grupo algébrico sobre $\mathbb{K}$, $(\mathbb{K}[G], \mu, u, \Delta, \varepsilon, S)$ sua álgebra Hopf de funções regulares e I_e seu ideal de aumento. Para todo $\varphi \in I_e$, $\Delta(\varphi) \in (1 \otimes \varphi + \varphi \otimes 1) + I_e \otimes I_e$.

Dem: Considere $\mathbb{K}[G] = \mathbb{K} + I_e$. Então

$$\Delta(\mathbb{K}[G] \otimes \mathbb{K}[G]) = \mathbb{K} \otimes \mathbb{K} + \mathbb{K} \otimes \mathbb{K}[G] + \mathbb{K}[G] \otimes \mathbb{K} + \mathbb{K}[G] \otimes \mathbb{K}[G].$$

Portanto é possível escrever $\Delta(\varphi)$ da seguinte forma

$$\Delta(\varphi) = k_1(1 \otimes 1) + k_2(1 \otimes \psi_1) + k_3(\psi_2 \otimes 1) + (\psi_3 \otimes \psi_4),$$

onde $k_1, k_2, k_3 \in \mathbb{K}$ e $\psi_1, \psi_2, \psi_3, \psi_4 \in I_e$. Usando o diagrama 1.3.4 da counidade, obtem-se que $(\varepsilon \otimes id) \circ \Delta = (id \otimes \varepsilon) \circ \Delta$ e ambos os termos são iguais a multiplicação escalar na álgebra $\mathbb{K}[G]$. Aplicando essa igualdade a φ, obtem-se que por um lado,

$$(\varepsilon \otimes id) \circ \Delta(\varphi) = k_1(1 \otimes 1) + k_2(1 \otimes \psi_1) = k_1 + k_2\psi_1$$

e por outro lado,

$$(id \otimes \varepsilon) \circ \Delta(\varphi) = k_1(1 \otimes 1) + k_3(\psi_2 \otimes 1) = k_1 + k_3\psi_2.$$

Ambos os lados são iguais a φ, portanto $k_1 = 0$, $k_2 = k_3 = 1$ e $\psi_1 = \psi_2 = \varphi$. Isso significa que $\Delta(\varphi) = (1 \otimes \varphi + \varphi \otimes 1) + (\psi_3 \otimes \psi_4)$, ou seja, $\Delta(\varphi) \in (1 \otimes \varphi + \varphi \otimes 1) + I_e \otimes I_e$. $\square$

Sejam G um grupo algébrico sobre $\mathbb{K}$, $(\mathbb{K}[G], \mu, u, \Delta, \varepsilon, S)$ sua álgebra de Hopf de funções regulares e $\mathcal{G} = Sp_{\mathbb{K}}\mathbb{K}[G]$ um esquema de grupo. Pela proposição 3.1.96, a cada morfismo de $\mathbb{K}$-álgebras corresponde um único morfismo dos correspondentes esquemas de grupos, em particular:

(i) À comultiplicação $\Delta : \mathbb{K}[G] \to \mathbb{K}[G] \otimes \mathbb{K}[G]$ corresponde uma transformação natural $m \in Hom(\mathcal{G} \times \mathcal{G}, \mathcal{G})$. Como $m \in Hom(\mathcal{G} \times \mathcal{G}, \mathcal{G})$, $m_A : \mathcal{G}(A) \times \mathcal{G}(A) \to \mathcal{G}(A)$ é um homomorfismo de grupos, para cada $A \in \mathbf{Alg}_{\mathbb{K}}$. Além disso, usando a coassociatividade de Δ é fácil mostrar que m_A é associativa.

(ii) À counidade $\varepsilon : \mathbb{K}[G] \to \mathbb{K}$ corresponde uma transformação natural $e \in Hom(\{0\}, \mathcal{G})$. Como $e \in Hom(\{0\}, \mathcal{G})$, para cada $A \in \mathbf{Alg}_{\mathbb{K}}$, $e_A : \{0\} \to \mathcal{G}(A)$. Além disso, usando as propriedades de counidade de ε, é fácil mostrar que $m_A \circ (e_A \otimes id_{\mathcal{G}(A)}) = m_A \circ (id_{\mathcal{G}(A)} \otimes e_A)$.

(iii) À antípoda $S : \mathbb{K}[G] \to \mathbb{K}[G]$ corresponde uma transformação natural $i \in Hom(\mathcal{G}, \mathcal{G})$. Como $i \in Hom(\mathcal{G}, \mathcal{G})$, para cada $A \in \mathbf{Alg}_{\mathbb{K}}$, $i_A : \mathcal{G}(A) \to \mathcal{G}(A)$. Além disso, usando as propriedades de antípoda de S, é fácil mostrar que $m_A \circ (i_A \otimes id_{\mathcal{G}(A)}) = m_A \circ (id_{\mathcal{G}(A)} \otimes i_A) = e_A$.

Portanto dado um grupo algébrico, existe um esquema de grupo algébrico e reduzido correspondente munido da estrutura acima. Por outro lado, a cada $\mathbb{K}$-esquema de grupo $\mathcal{G}$ algébrico e reduzido corresponde um grupo algébrico, a saber, $\mathcal{G}(\mathbb{K})$. É fácil ver que a estrutura de grupo de $\mathcal{G}(\mathbb{K})$, como descrita acima, coincide com a estrutura de grupo de G ([Jan], p.21).

4.3.2 Álgebra de distribuições

Na seção 3.3 foram definidos o ideal de aumento e, a partir dele, a coálgebra de distribuições de uma variedade algébrica. No caso de grupos algébricos, as coálgebras de distribuição são de fato álgebras de Hopf. Considere $\mathbb{K}$ um corpo algebricamente fechado.

Definição 4.3.5. Seja G um grupo algébrico sobre $\mathbb{K}$. Defina as *distribuições de* G, $D(G)$, como as distribuições da variedade G com suporte na identidade do grupo. Ou seja, $D(G) = D(G, e) = \{\varphi \in \mathbb{K}[G]^* \mid \exists\, m \in \mathbb{N}, \varphi(I_e^{m+1}) = 0\}$.

O conjunto de distribuições de um grupo algébrico é munido de uma estrutura de álgebra de Hopf. Essa estrutura é descrita a seguir.

Denote por $\mu : \mathbb{K}[G] \times \mathbb{K}[G] \to \mathbb{K}[G]$ a multiplicação da álgebra de funções regulares de G, por $u : \mathbb{K} \to \mathbb{K}[G]$ a sua unidade, por $\Delta : \mathbb{K}[G] \to \mathbb{K}[G] \otimes \mathbb{K}[G]$ sua comultiplicação, por $\varepsilon : \mathbb{K}[G] \to \mathbb{K}$ sua counidade e por $S : \mathbb{K}[G] \to \mathbb{K}[G]$ sua antípoda.

A multiplicação $\mu_d = \Delta^* : D(G) \otimes D(G) \to D(G)$ é dada da seguinte forma: para quaisquer $\varphi, \psi \in D(G)$,

$$\mu_d(\varphi \otimes \psi)(f) = (\varphi \otimes \psi)(\Delta(f)),$$

para todo $f \in \mathbb{K}[G]$. Essa multiplicação é associativa. De fato, dados $\varphi, \psi, \xi \in D[G]$ e $f \in \mathbb{K}[G]$,

$$\begin{aligned} \mu_d \circ (id \otimes \mu_d)(\varphi \otimes \psi \otimes \xi)(f) &= (id \otimes \mu_d)(\varphi \otimes \psi \otimes \xi)(\Delta(f)) \\ &= (\varphi \otimes \psi \otimes \xi)((id \otimes \Delta) \circ \Delta)(f). \end{aligned}$$

Por outro lado,

$$\begin{aligned}\mu_d \circ (\mu_d \otimes id)(\varphi \otimes \psi \otimes \xi)(f) &= (\mu_d \otimes id)(\varphi \otimes \psi \otimes \xi)(\Delta(f))\\ &= (\varphi \otimes \psi \otimes \xi)((\Delta \otimes id) \circ \Delta)(f).\end{aligned}$$

Como a comultiplicação de $\mathbb{K}[G]$ é coassociativa, $\mu_d \circ (id \otimes \mu_d) = \mu_d \circ (\mu_d \otimes id)$.

A unidade $u_d = \varepsilon^* : \mathbb{K} \to D(G)$ é tal que, para cada $k \in \mathbb{K}$, $u_d(k)(f) = kf(e)$ para todo $f \in \mathbb{K}[G]$. Para quaisquer $k \in \mathbb{K}$, $\varphi \in D(G)$ e $f \in \mathbb{K}[G]$,

$$\begin{aligned}\mu_d \circ (u_d \otimes id)(k \otimes \varphi)(f) &= (u_d \otimes id)(k \otimes \varphi)(\Delta(f))\\ &= k(1 \otimes \varphi)(((\varepsilon \otimes id) \circ \Delta)(f))\\ &= k\varphi(f)(\text{pela propriedade 1.3.1 da counidade})\\ &e\\ \mu_d \circ (id \otimes u_d)(\varphi \otimes k)(f) &= (id \otimes u_d)(\varphi \otimes k)(\Delta(f))\\ &= k(\varphi \otimes 1)(((id \otimes \varepsilon) \circ \Delta)(f))\\ &= k\varphi(f)(\text{pela propriedade 1.3.1 da counidade}).\end{aligned}$$

Isso mostra que os diagramas de unidade (1.3.1) são comutativos.

A comultiplicação e a counidade são herdadas da estrutura de coálgebra do conjunto de distribuições e já foram descritas na seção 3.3.

Para completar a estrutura de álgebra de Hopf, a antípoda $S_d = S^* : D(G) \to D(G)$ é dada da seguinte forma $S_d(\varphi) = \varphi \circ S$, para cada $\varphi \in D(G)$. Então

$$\begin{aligned}\mu_d \circ (S_d \otimes id) \circ \Delta_d(\varphi) &= \mu_d \circ (S_d \otimes id)(\varphi \circ \mu)\\ &= \mu_d(\varphi \circ \mu \circ (S \otimes id))\\ &= \varphi \circ \mu \circ (S \otimes id) \circ \Delta\\ &= \varphi \circ u \circ \varepsilon\\ &= u_d(\varphi \circ u)\\ &= (u_d \circ \varepsilon_d)(\varphi)\\ &e\\ \mu_d \circ (id \otimes S_d) \circ \Delta_d(\varphi) &= \mu_d \circ (id \otimes S_d)(\varphi \circ \mu)\\ &= \mu_d(\varphi \circ \mu \circ (id \otimes S))\\ &= \varphi \circ \mu \circ (id \otimes S) \circ \Delta\\ &= \varphi \circ u \circ \varepsilon\\ &= u_d(\varphi \circ u)\\ &= (u_d \circ \varepsilon_d)(\varphi).\end{aligned}$$

Isso mostra que

$$\mu_d \circ (S_d \otimes id) \circ \Delta_d = u_d \circ \varepsilon_d = \mu_d \circ (id \otimes S_d) \circ \Delta_d,$$

ou seja, os diagramas (1.3.4) da aplicação antípoda são comutativos.

Exemplo 4.3.6. Considere o grupo aditivo $G_a(\mathbb{K})$. Como descrito no exemplo 3.3.12, a álgebra de distribuições de $G_a(\mathbb{K})$ é $\{f \in \mathbb{K}[x]^* \mid \exists\ m \in \mathbb{N}, \text{tal que } f(x^m) = 0\}$, ou seja, $D(G_a)$ é o $\mathbb{K}$-espaço gerado pelos funcionais x_i, $i \in \mathbb{N}$, onde

$$x_i(x^j) = \delta_{ij}, \quad i, j \in \mathbb{N}.$$

A multiplicação da álgebra de Hopf $D(G_a)$ é dada por um lado por

$$\mu_d(x_i, x_j)(x^n) = \sum_{k\geq 0} c_k x_k(x^n) = c_n,$$

para alguns $c_k \in \mathbb{K}, \forall\, i, j, n \in \mathbb{N}$, e por outro lado por

$$\begin{aligned}\mu_d(x_i, x_j)x^n &= (x_i \otimes x_j)(\Delta(x^n))\\ &= (x_i \otimes x_j)\left(\sum_{l=0}^{n}\binom{n}{l}x^l \otimes x^{n-l}\right)\\ &= \sum_{l=0}^{n}\binom{n}{l}x_i(x^l)x_j(x^{n-l})\\ &= \binom{n}{l}\delta_{i,l}\delta_{j,n-l}.\end{aligned}$$

Portanto $c_n = \binom{n}{l}$, quando $n = i + j$ e $l = i$. Isso mostra que

$$\mu_d(x_i, x_j) = \binom{i+j}{i}x_{i+j}, \quad \forall\, i, j \in \mathbb{N}.$$

A unidade é por definição $u_d(k) = k \circ \varepsilon$. Consequentemente, para todo $k \in \mathbb{K}$ e $n \in \mathbb{N}$,

$$u_d(k)(x^n) = k\varepsilon(x^n) = k\delta_{0,n}.$$

Portanto $u_d(k) = kx_0$, $\forall\, k \in \mathbb{K}$.

A comultiplicação é dada por

$$\Delta_d(x_k) = \sum_{l=0}^{n} x_l \otimes x_{k-l}, \quad k \in \mathbb{N}^{\bullet}.$$

Enquanto a counidade é dada por

$$\varepsilon_d(x_0) = 1 \quad e \quad \varepsilon_d(x_n) = 0, \quad n \in \mathbb{N}^{\bullet}.$$

A antípoda, por sua vez, é por definição $S_d(x_k) = x_k \circ S$. Consequentemente, para cada $n \in \mathbb{N}$,

$$(x_k \circ S)(x^n) = x_k((-x)^n) = (-1)^k\delta_{k,n}.$$

Portanto $S_d(x_k) = (-1)^k x_k$, $k \in \mathbb{N}$.

Exemplo 4.3.7. Considere o grupo multiplicativo $G_m(\mathbb{K})$. Como descrito no exemplo 3.3.12, a álgebra de distribuições de $G_m(\mathbb{K})$ é, o $\mathbb{K}$-espaço gerado pelos funcionais t_i, $i \in \mathbb{N}$, onde $t_i((t-1)^j) = \delta_{ij}$, para cada $i, j \in \mathbb{Z}$.

A multiplicação da álgebra de Hopf $D(G_m)$ é dada por um lado por

$$\mu_d(t_i, t_j)((t-1)^n) = \sum_{k\in\mathbb{Z}} c_k t_k((t-1)^n) = c_n$$

para alguns $c_k \in \mathbb{K}, i, j \in \mathbb{N}, n \in \mathbb{Z}$ e por outro lado por

$$\begin{aligned}
\mu_d(t_i, t_j)((t-1)^n) &= (t_i \otimes t_j)(\Delta((t-1)^n)) \\
&= (t_i \otimes t_j)\left(\sum_{0\le l\le m\le n} \binom{n}{m}\binom{m}{l}(t-1)^{n-l} \otimes (t-1)^{n+l-m}\right) \\
&= \sum_{0\le l\le m\le n} \binom{n}{m}\binom{m}{l} t_i((t-1)^{n-l}) \otimes t_j((t-1)^{n+l-m}).
\end{aligned}$$

Isso faz com que

$$\begin{aligned}
c_{l+i} &= \sum_{0\le l\le m\le l+i} \binom{l+i}{m}\binom{m}{l} t_j((t-1)^{2l+i-m}) \\
&= \sum_{0\le r\le i} \binom{l+i}{l+r}\binom{l+r}{l} t_j((t-1)^{l+i-r}) \\
&= \sum_{0\le l\le m\le l+i} \binom{l+i}{m}\binom{m}{l} \delta_{j+r,l+i}.
\end{aligned}$$

Portanto

$$\mu_d(t_i, t_j) = \sum_{0\le k\le i,j} \binom{i+j-k}{j}\binom{j}{k} t_{i+j-k}.$$

A unidade é por definição $u_d(k) = k \circ \varepsilon$. Consequentemente, para todo $k \in \mathbb{K}$ e $n \in \mathbb{N}$,

$$u_d(k)((t-1)^n) = k\varepsilon((t-1)^n) = k\delta_{0,n}.$$

Portanto, $u_d(k) = kt_0$, $\forall\ k \in \mathbb{K}$.

A comultiplicação é

$$\Delta_d(t_k) = \sum_{l=0}^{n} t_l \otimes t_{k-l}, \quad \forall\ k \in \mathbb{N}.$$

Enquanto a counidade é dada por

$$\varepsilon_d(t_0) = 1, \quad \varepsilon_d(t_i) = 0, i \in \mathbb{N}^\bullet.$$

A antípoda, por sua vez, é por definição $S_d(t_k) = t_k \circ S$. Consequentemente, para cada $k, l \in \mathbb{N}$,

$$(t_k \circ S)(t^l) = t_k(t^{-l}) = (-1)^k \delta_{k,l}.$$

Portanto,

$$S_d(t_k) = (-1)^k t_k, \quad \forall\ k \in \mathbb{N}.$$

Proposição 4.3.8. A álgebra de distribuições de um grupo algébrico G é uma álgebra associativa filtrada, cuja n-ésima filtração é $D_n(G, e)$.

Dem: A afirmação diz que $D(G) = \bigcup_{n\in\mathbb{N}} D_n(G, e)$ é uma filtração. Para mostrar isso basta mostrar que $D_n(G, e)D_m(G, e) \subseteq D_{n+m}(G, e)$. Ou seja, basta mostrar que se $\varphi \in D_n(G, e)$ e $\psi \in D_m(G, e)$, então $\mu_d(\varphi, \psi) \in D_{n+m}(G, e)$. De fato, usando a proposição 4.3.4,

$$\Delta(I_e^\nu) \subseteq \sum_{\nu\le k,l\le 2\nu} I_e^k \otimes I_e^l.$$

Portanto, tomando $\nu = n + m + 1$, $\mu_d(\varphi, \psi)(I_e^{n+m+1}) = 0$. □

4.4 Hiperálgebras

Durante esta seção, considere $\mathfrak{g}$ uma álgebra de Lie semissimples e de dimensão finita sobre um corpo $\mathbb{K}$ de característica zero e algebricamente fechado. Considere também $\mathfrak{h}$ uma subálgebra toral maximal de $\mathfrak{g}$, $\mathcal{R}$ um sistema de raizes de $\mathfrak{g}$ e $\mathsf{B} = \{\mathsf{y}_\alpha, \mathsf{h}_i, \mathsf{x}_\alpha \mid \alpha \in \mathcal{R}^+ \ e \ i = 1, \ldots, \dim \mathfrak{h}\}$ uma base de Chevalley de $\mathfrak{g}$, como descrito no capítulo 2.

Definição 4.4.1. Defina $\mathfrak{g}_\mathbb{Z}$ como o reticulado de $\mathfrak{g}$ $\mathbb{Z}$-gerado pela base de Chevalley B. Para todo corpo algebricamente fechado $\mathbb{F}$, defina a $\mathbb{F}$-*álgebra de Chevalley* de $\mathfrak{g}$ como $\mathfrak{g}_\mathbb{F} = \mathbb{F} \otimes_\mathbb{Z} \mathfrak{g}_\mathbb{Z}$.

Considerando a representação adjunta, uma álgebra de Lie $\mathfrak{g}$ pode ser vista como um $\mathfrak{g}$-módulo. Dessa forma, como $\mathfrak{g}_\mathbb{Z}$ é gerado pela base de Chevalley, $\mathfrak{g}_\mathbb{Z}$ pode ser visto como um $\mathfrak{g}_\mathbb{Z}$-submódulo de $\mathfrak{g}$. Ainda mais, $\mathfrak{g}_\mathbb{F}$ é uma álgebra de Lie sobre $\mathbb{F}$ e $\mathfrak{g}_\mathbb{Z}$ é um reticulado admissível de $\mathfrak{g}$. Em particular, $\mathfrak{g}_\mathbb{K} \simeq \mathfrak{g}$.

Definição 4.4.2. Sejam $U(\mathfrak{g})_\mathbb{Z}$ a forma integral de Kostant de $\mathfrak{g}$ e $\mathbb{F}$ um corpo. Defina a $\mathbb{F}$-*hiperálgebra de* $\mathfrak{g}$ como $U(\mathfrak{g})_\mathbb{F} = \mathbb{F} \otimes_\mathbb{Z} U(\mathfrak{g})_\mathbb{Z}$.

A forma integral de Kostant $(U(\mathfrak{g})_\mathbb{Z}, \mu_U, u_U, \Delta_U, \varepsilon_U, S_U)$ é uma álgebra de Hopf com a estrutura herdada de $U(\mathfrak{g})$.

Exemplo 4.4.3. Considere a base de Chevalley de $\mathfrak{sl}_2(\mathbb{C})$ dada por $\{\mathsf{y}, \mathsf{h}, \mathsf{x}\}$.

A multiplicação em $U(\mathfrak{sl}_2)_\mathbb{Z}$ é dada por:

$$\begin{aligned}
\mathsf{x}^{(i)}.\mathsf{x}^{(j)} &= \binom{i+j}{i}\mathsf{x}^{(i+j)} \\
\mathsf{y}^{(i)}.\mathsf{y}^{(j)} &= \binom{i+j}{i}\mathsf{y}^{(i+j)} \\
\binom{\mathsf{h}}{i}.\binom{\mathsf{h}}{j} &= \sum_{0 \le k \le i,j} \binom{i+j-k}{i+j-2k}\binom{i+j-2k}{j-k}\binom{\mathsf{h}}{i+j-k} \\
\mathsf{x}^{(i)}.\mathsf{y}^{(j)} &= \sum_{0 \le k \le i,j} \mathsf{y}^{(j-k)}.\binom{\mathsf{h}-(i+j-2k)}{k}.\mathsf{x}^{(i-k)} \\
\binom{\mathsf{h}}{k}.\mathsf{x}^{(i)} &= \mathsf{x}^{(i)}.\binom{\mathsf{h}+2i}{k} \\
\binom{\mathsf{h}}{k}.\mathsf{y}^{(i)} &= \mathsf{y}^{(i)}.\binom{\mathsf{h}-2i}{k}.
\end{aligned}$$

A unidade é dada por:

$$\begin{aligned}
u : \mathbb{Z} &\longrightarrow U(\mathfrak{sl}_2)_\mathbb{Z} \\
n &\longrightarrow n.1
\end{aligned}$$

A comultiplicação é dada por:

$$\Delta(\mathsf{x}^{(k)}) = \sum_{i=0}^{k} \mathsf{x}^{(i)} \otimes \mathsf{x}^{(k-i)}$$
$$\Delta(\mathsf{y}^{(k)}) = \sum_{i=0}^{k} \mathsf{y}^{(i)} \otimes \mathsf{y}^{(k-i)}$$
$$\Delta\binom{\mathsf{h}}{k} = \sum_{i=0}^{k} \binom{\mathsf{h}}{i} \otimes \binom{\mathsf{h}}{k-i}.$$

A counidade é dada por:

$$\varepsilon(\mathsf{x}^{(i)}) = \delta_{0,i}$$
$$\varepsilon(\mathsf{y}^{(j)}) = \delta_{0,j}$$
$$\varepsilon\binom{\mathsf{h}}{k} = \delta_{0,k}.$$

A antípoda é dada por:

$$S(\mathsf{x}^{(i)}) = (-1)^i \mathsf{x}^{(i)}$$
$$S(\mathsf{y}^{(j)}) = (-1)^j \mathsf{y}^{(j)}$$
$$S\binom{\mathsf{h}}{k} = (-1)^k \binom{\mathsf{h}}{k}.$$

Como para cada $\alpha \in \mathcal{R}^+$, a subálgebra de $\mathfrak{g}$ gerada por $\{\mathsf{y}_\alpha, \mathsf{h}_\alpha, \mathsf{x}_\alpha\}$ é isomorfa a $\mathfrak{sl}_2$, o exemplo acima mostra a seguinte proposição.

Proposição 4.4.4. A multiplicação em $U(\mathfrak{g})_{\mathbb{Z}}$ satisfaz:

$$\mathsf{x}_\alpha^{(k)}.\mathsf{x}_\alpha^{(l)} = \binom{k+l}{k} \mathsf{x}_\alpha^{(k+l)}$$
$$\mathsf{y}_\alpha^{(k)}.\mathsf{y}_\alpha^{(l)} = \binom{k+l}{k} \mathsf{y}_\alpha^{(k+l)}$$
$$\binom{\mathsf{h}_i}{r}.\binom{\mathsf{h}_i}{s} = \sum_{0 \leq k \leq r,s} \binom{r+s-k}{r+s-2k}\binom{r+s-2k}{s-k}\binom{\mathsf{h}_i}{r+s-k}$$
$$\mathsf{x}_\alpha^{(r)}.\mathsf{y}_\alpha^{(s)} = \sum_{0 \leq k \leq r,s} \mathsf{y}_\alpha^{(s-k)}.\binom{\mathsf{h}_\alpha - (r+s-2k)}{k}.\mathsf{x}_\alpha^{(r-k)}$$
$$\binom{\mathsf{h}_i}{k}.\mathsf{x}_\alpha^{(l)} = \mathsf{x}_\alpha^{(l)}.\binom{\mathsf{h}_i + \alpha(h_i)l}{k}$$
$$\binom{\mathsf{h}_i}{k}.\mathsf{y}_\alpha^{(l)} = \mathsf{y}_\alpha^{(l)}.\binom{\mathsf{h}_i - \alpha(h_i)l}{k}.$$

A unidade é dada por:

$$\begin{aligned} u : \mathbb{Z} &\longrightarrow U(\mathfrak{g})_{\mathbb{Z}} \\ n &\longrightarrow n.1 \end{aligned}$$

A comultiplicação é dada por:

$$\Delta(\mathsf{x}_\alpha^{(k)}) = \sum_{i=0}^{k} \mathsf{x}_\alpha^{(i)} \otimes \mathsf{x}_\alpha^{(k-i)}$$
$$\Delta(\mathsf{y}_\alpha^{(k)}) = \sum_{j=0}^{k} \mathsf{y}_\alpha^{(j)} \otimes \mathsf{y}_\alpha^{(k-j)}$$
$$\Delta\binom{\mathsf{h}_i}{k} = \sum_{j=0}^{k} \binom{\mathsf{h}_i}{j} \otimes \binom{\mathsf{h}_i}{k-j}.$$

A counidade é dada por:

$$\varepsilon(\mathsf{x}_\alpha^{(j)}) = \delta_{0,j}$$
$$\varepsilon(\mathsf{y}_\alpha^{(j)}) = \delta_{0,j}$$
$$\varepsilon\binom{\mathsf{h}_i}{k} = \delta_{0,k}.$$

A antípoda é dada por:

$$S(\mathsf{x}_\alpha^{(j)}) = (-1)^j \mathsf{x}_\alpha^{(j)}$$
$$S(\mathsf{y}_\alpha^{(j)}) = (-1)^j \mathsf{y}_\alpha^{(j)}$$
$$S\binom{\mathsf{h}_i}{k} = (-1)^k \binom{\mathsf{h}_i}{k}.$$

Consequentemente as $\mathbb{F}$-hiperálgebras são álgebras de Hopf sobre o corpo $\mathbb{F}$. Explicitamente:

(*i*) $\mu(f_1 \otimes \varphi_1, f_2 \otimes \varphi_2) = f_1 f_2 \otimes \mu_U(\varphi_1, \varphi_2)$;

(*ii*) $u(f \otimes \varphi) = f u_U(\varphi)$;

(*iii*) $\Delta(f \otimes \varphi) = f \Delta_U(\varphi)$;

(*iv*) $\varepsilon(f \otimes \varphi) = f \varepsilon_U(\varphi)$;

(*v*) $S(f \otimes \varphi) = f S_U(\varphi)$.

A $\mathbb{K}$-hiperálgebra de $\mathfrak{g}$ é isomorfa (como álgebra de Hopf) a álgebra universal envelopante $U(\mathfrak{g})$.

Proposição 4.4.5. Sejam $\mathfrak{g}$ uma álgebra de Lie semissimples sobre $\mathbb{K}$ com matriz de Cartan $A = (a_{ij})$, $1 \leq i, j \leq l$, e $\mathbb{F}$ um corpo algebricamente fechado. A hiperálgebra $U(\mathfrak{g})_{\mathbb{F}}$ é a álgebra gerada pelo conjunto $\{h_i^{(n)}, x_i^{(n)}, y_i^{(n)} \mid 1 \leq i \leq l,\ n \in \mathbb{N}\}$ satisfazendo as seguintes relações:

(*i*) $h_i^{(0)} = x_i^{(0)} = y_i^{(0)} = 1, \forall\ 1 \leq i \leq l,$

(*ii*) $h_i(t)h_i(u) = h_i(t + u + tu), \forall\ 1 \leq i \leq l,$

(iii) $h_i(t)h_j(u) = h_j(u)h_i(t), \forall\ 1 \leq i, j \leq l,$

(iv) $x_i(t)x_i(u) = x_i(t+u),\ y_i(t)y_i(u) = y_i(t+u), \forall\ 1 \leq i \leq l,$

(v) $x_i(t)y_i(u) = y_i\left(\frac{u}{tu+1}\right)h_i(tu)x_i\left(\frac{t}{tu+1}\right), \forall\ 1 \leq i \leq l,$

(vi) $x_i(t)y_j(u) = y_j(u)x_i(t), \forall\ 1 \leq i \neq j \leq l,$

(vii) $h_i(t)x_j(u)h_i(t)^{-1} = x_j((t+1)^{a_{ij}}u), \forall\ 1 \leq i, j \leq l,$

$(viii)$ $h_i(t)y_j(u)h_i(t)^{-1} = y_j((t+1)^{-a_{ij}}u), \forall\ 1 \leq i, j \leq l,$

(ix) $ad\left(x_i^{(n)}\right)\left(x_j^{(m)}\right) = \sum_{k=0}^{n}(-1)^k x_i^{(n-k)}x_j^{(m)}x_i^{(k)} = 0$, se $n + ma_{ij} > 0, \forall\ 1 \leq i \neq j \leq l,$

(x) $ad\left(y_i^{(n)}\right)\left(y_j^{(m)}\right) = \sum_{k=0}^{n}(-1)^k y_i^{(n-k)}y_j^{(m)}y_i^{(k)} = 0$, se $n + ma_{ij} > 0, \forall\ 1 \leq i \neq j \leq l,$

onde

$$h_i(t) = \sum_{n=0}^{\infty} t^n h_i^{(n)} \quad x_i(t) = \sum_{n=0}^{\infty} t^n x_i^{(n)} \quad y_i(t) = \sum_{n=0}^{\infty} t^n y_i^{(n)}$$

pertencem a $U(\mathfrak{g})_{\mathbb{F}}[[t]]$ e as relações $(i) - (viii)$ são igualdades em $U(\mathfrak{g})_{\mathbb{F}}[[t, u]]$.

Dem: Explicitamente o isomorfismo é dado por:

$$\begin{aligned} x_i^{(k)} &\mapsto x_{\alpha_i}^k \\ y_i^{(k)} &\mapsto y_{\alpha_i}^k \\ h_i^{(k)} &\mapsto \binom{h_i}{k}. \end{aligned}$$

A demonstração de que a função acima é isomorfismo é bastante sofisticada e extensa. Ela está feita no artigo [Tak2]. □

4.5 Grupos de Chevalley

Durante essa seção, considere $\mathfrak{g}$ uma álgebra de Lie semissimples e de dimensão finita sobre um corpo $\mathbb{K}$ algebricamente fechado e de característica zero. Considere $\mathfrak{h}$ uma subálgebra de Cartan, $\mathcal{R}$ um sistema de raízes e $\mathsf{B} = \{\mathsf{y}_\alpha, \mathsf{h}_i, \mathsf{x}_\alpha \mid \alpha \in \mathcal{R}^+,\ i = 1, \ldots, \dim \mathfrak{h}\}$ uma base de Chevalley de $\mathfrak{g}$. Considere uma representação fiel de $\mathfrak{g}$ de dimensão finita $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$. Considere $\mathbb{F}$ um corpo algebricamente fechado.

Se $\mathcal{L}_{\mathbb{Z}}$ é um reticulado admissível de V, então a representação ρ induz uma representação $\rho : U(\mathfrak{g})_{\mathbb{Z}} \to \mathfrak{gl}(\mathcal{L}_{\mathbb{Z}})$. Considere $\mathcal{L}_{\mathbb{F}} = \mathbb{F} \otimes_{\mathbb{Z}} \mathcal{L}_{\mathbb{Z}}$. Como $U(\mathfrak{g})_{\mathbb{F}} = \mathbb{F} \otimes_{\mathbb{Z}} U(\mathfrak{g})_{\mathbb{Z}}$, a representação ρ induz uma representação $\rho : U(\mathfrak{g})_{\mathbb{F}} \to \mathfrak{gl}(\mathcal{L}_{\mathbb{F}})$. Explicitamente, $\rho(k \otimes \mathsf{x}) = k \otimes \rho(\mathsf{x})$ para todo $k \in \mathbb{F}, \mathsf{x} \in U(\mathfrak{g})_{\mathbb{Z}}$.

Observe que pelo fato da representação (V, ρ) ter dimensão finita e por 2.3.13, para todo $\alpha \in \mathcal{R}^+$, existe $n_\alpha \in \mathbb{N}$, tal que $\rho(\mathsf{x}_\alpha^{(n)}) = 0$ para todo $n \geq n_\alpha$. Analogamente existe $n_{-\alpha} \in \mathbb{N}$, tal que $\rho(\mathsf{y}_\alpha^{(n)}) = 0$ para todo $n \geq n_{-\alpha}$.

Definição 4.5.1. Sejam $\alpha \in \mathcal{R}^+$ e $k \in \mathbb{F}$. Defina

$$\exp(k\mathsf{x}_\alpha) = \sum_{n\in\mathbb{N}} k^n \rho\left(\mathsf{x}_\alpha^{(n)}\right) \in Sl(\mathcal{L}_\mathbb{F}),$$
$$\exp(k\mathsf{y}_\alpha) = \sum_{n\in\mathbb{N}} k^n \rho\left(\mathsf{y}_\alpha^{(n)}\right) \in Sl(\mathcal{L}_\mathbb{F}).$$

Por simplicidade, denote $\exp(k\mathsf{x}_\alpha)$ por $x_\alpha(k)$ e $\exp(k\mathsf{y}_\alpha)$ por $x_{-\alpha}(k)$. Defina o grupo $\mathfrak{X}_\alpha(\mathbb{F})$ como o grupo gerado por $\{x_\alpha(k) \mid k \in \mathbb{F}\}$, onde $\alpha \in \mathcal{R}$.

Observe que a notação introduzida para os grupos $\mathfrak{X}_\alpha(\mathbb{F})$ não deixa explícita a representação usada para construir cada uma das exponenciais $x_\alpha(k) \in \mathfrak{X}_\alpha(\mathbb{F})$. Contudo a construção desses grupos depende fortemente da representação utilizada. Isso porém, não deve causar confusão.

Considere $\mathfrak{X}_\alpha(\mathbb{F})$ munido da estrutura de grupo cuja multiplicação é $x_\alpha(k_1)x_\alpha(k_2) = x_\alpha(k_1 + k_2)$, $\forall\ k_1, k_2 \in \mathbb{F}$. A identidade do grupo é $x_\alpha(0)$ e $(x_\alpha(k))^{-1} = x_\alpha(-k)$, $\forall\ k \in \mathbb{F}$. Com essa estrutura, a seguinte proposição se torna clara.

Proposição 4.5.2. Os grupos $\mathfrak{X}_\alpha(\mathbb{F})$, $\alpha \in \mathcal{R}$, são isomorfos a $G_a(\mathbb{F})$ (como grupos).

Como os grupos aditivos $G_a(\mathbb{F})$ são algébricos, é natural se perguntar se os grupos $\mathfrak{X}_\alpha(\mathbb{F})$, $\alpha \in \mathcal{R}$, também são algébricos. Considere $Y \subseteq \mathfrak{X}_\alpha(\mathbb{F})$, $\alpha \in \mathcal{R}$, uma variedade algébrica em $\mathfrak{X}_\alpha(\mathbb{F})$ quando $Y = \{x_\alpha(k) \mid k \in X\text{: variedade algébrica de } G_a(\mathbb{F})\}$. Usando o isomorfismo da proposição 4.5.2, a seguinte proposição se torna clara.

Proposição 4.5.3. Os grupos algébricos $\mathfrak{X}_\alpha(\mathbb{F})$, $\alpha \in \mathcal{R}$, são isomorfos a $G_a(\mathbb{F})$ (como grupos algébricos).

Definição 4.5.4. Seja $\Lambda(V, \rho) = \Lambda$. Defina o *Grupo de Chevalley* do tipo Λ como o grupo $G(\mathfrak{g}, \mathbb{F}, \Lambda)$ gerado por

$$\{x_\alpha(k) = \sum_{n\in\mathbb{N}} k^n \rho\left(\mathsf{x}_\alpha^{(n)}\right) \mid k \in \mathbb{F},\ \alpha \in \mathcal{R}\}.$$

$G(\mathfrak{g}, \mathbb{F}, \mathcal{Q})$ é chamado de *Grupo de Chevalley Adjunto* e $G(\mathfrak{g}, \mathbb{F}, \mathcal{P})$ é chamado de *Grupo de Chevalley Universal*.

Como consequência da proposição 4.5.3, do fato de que o grupo de Chevalley é gerado pelos grupos algébricos $\mathfrak{X}_\alpha(\mathbb{F})$, $\alpha \in \mathcal{R}$, e da proposição 4.1.11, obtem-se a seguinte proposição.

Proposição 4.5.5. Os grupos de Chevalley são algébricos.

Exemplo 4.5.6.

(i) $G(\mathfrak{sl}_n, \mathbb{F}, \mathcal{P}) \simeq Sl_n(\mathbb{F})$.

(ii) $G(\mathfrak{so}_n, \mathbb{F}, \mathcal{P})$ é isomorfo ao grupo derivado de $SO_n(\mathbb{F})$.

(iii) $G(\mathfrak{sp}_{2n}, \mathbb{F}, \mathcal{P}) \simeq Sp_{2n}(\mathbb{F})$.

Os exemplos anteriores são descritos em [Ree].

Considere G um grupo algébrico semissimples sobre $\mathbb{K}$ e $\mathfrak{g}$ a álgebra de Lie de G. Como a álgebra de Lie de G é uma álgebra de Lie semissimples sobre $\mathbb{K}$, a definição 4.5.4 associa a G uma família de grupos de Chevalley universais $G(\mathfrak{g}, \mathbb{F}, \mathcal{P})$. Essa família é parametrizada pelos corpos $\mathbb{F}$. Denote $G(\mathfrak{g}, \mathbb{F}, \mathcal{P})$ por $G_{\mathbb{F}}$ quando tal notação não causar confusão.

A construção da família $G_{\mathbb{F}}$ é feita a partir da $\mathbb{Z}$-álgebra $U(\mathfrak{g})_{\mathbb{Z}}$. Por um lado, para cada corpo $\mathbb{F}$, tem-se $\mathbb{F} \otimes_{\mathbb{Z}} U(\mathfrak{g})_{\mathbb{Z}} = U(\mathfrak{g})_{\mathbb{F}}$. Por outro lado, cada um dos grupos algébricos $G_{\mathbb{F}}$ está associado a uma $\mathbb{F}$-álgebra, a saber, a álgebra de funções regulares $\mathbb{F}[G_{\mathbb{F}}]$. Por esses dois fatos, seria natural tentar definir uma $\mathbb{Z}$-álgebra de Hopf $\mathbb{Z}[G]$ que fosse análoga a uma álgebra afim, ou seja, que fosse uma $\mathbb{Z}$-álgebra finitamente gerada, comutativa e reduzida, tal que para cada corpo $\mathbb{F}$, $\mathbb{F} \otimes_{\mathbb{Z}} \mathbb{Z}[G] \simeq \mathbb{F}[G_{\mathbb{F}}]$.

Definição 4.5.7. Seja A uma álgebra de Hopf e seja $I \subseteq A$ um ideal. Diz-se que I é um *ideal de tipo finito* quando A/I for um $\mathbb{Z}$-módulo finitamente gerado e livre, ou seja, $A/I = \mathbb{Z}^n$, $n < \infty$.

Sejam I, J dois ideais de tipo finito em A. Considere $\pi_I : A \to A/I$ e $\pi_J : A \to A/J$ os morfismos sobrejetores canônicos de álgebras de Hopf e defina $I \wedge J$ como o núcleo do morfismo $(\pi_I \otimes \pi_J) \circ \Delta : A \to A/I \otimes A/J$.

Seja $\mathcal{F}$ uma família de ideais de A de tipo finito. A família $\mathcal{F}$ é chamada de *admissível* quando:

(i) $\bigcap_{I \in \mathcal{F}} I = \langle 0 \rangle$,

(ii) $\mathcal{F}$ é fechado quanto a antípoda de A, ou seja, $S_A(I) \in \mathcal{F}$, $\forall\, I \in \mathcal{F}$,

(iii) $\mathcal{F}$ é fechado quanto a $\wedge$, ou seja, $(I \wedge J) \in \mathcal{F}$, $\forall\, I, J \in \mathcal{F}$.

Seja $\mathcal{F}$ uma família admissível de ideiais de A. Defina a álgebra

$$A_{\mathcal{F}} = \{f \in Hom_{Alg_{\mathbb{Z}}}(A, \mathbb{Z}) \mid \exists\, I \in \mathcal{F}, f(I) = 0\}.$$

Exemplo 4.5.8. Considere A uma álgebra de Hopf e $I \subseteq A$ um ideal de tipo finito. Considere $\mathcal{F}$ como a família de ideais $\mathcal{F} = \{I^n \mid n \in \mathbb{N}^\bullet\}$. A família $\mathcal{F}$ é admissível. Em particular, as álgebras de distribuições de grupos algébricos são da forma $A_{\mathcal{F}}$.

Considere G um grupo algébrico sobre $\mathbb{K}$ e $\rho : G \to Gl(V)$ uma representação racional de G de dimensão finita. Diferenciando essa representação, obtem-se uma representação de dimensão finita da álgebra de Lie $\mathfrak{g}$, a saber, $d\rho : \mathfrak{g} \to \mathfrak{gl}(V)$. Como $U(\mathfrak{g})$ é a álgebra universal envelopante de $\mathfrak{g}$, $d\rho$ induz uma representação de dimensão finita de $U(\mathfrak{g})$. Denote essa representação por $\varphi : U(\mathfrak{g}) \to \mathfrak{gl}(V)$.

A construção acima é natural e associa a cada representação de dimensão finita de G uma representação de dimensão finita de $U(\mathfrak{g})$.

Considere agora a coleção das classes de equivalência de representações de dimensão finita de G, onde $\rho_1 : G \to Gl(V_1)$ é equivalente a $\rho_2 : G \to Gl(V_2)$, quando existe um isomorfismo linear $\varphi : V_1 \to V_2$, tal que $\varphi(\rho_1(g)(v_1)) = \rho_2(g)(\varphi(v_1))$ para todo $g \in G$ e $v_1 \in V_1$. Considere a coleção das classes de equivalência de representações de $U(\mathfrak{g})$ induzidas. Considere a família $\widetilde{\mathcal{F}}$ dos núcleos de tais representações induzidas. Defina a família $\mathcal{F}$ como $\mathcal{F} = \{I \cap U(\mathfrak{g})_{\mathbb{Z}} \mid I \in \widetilde{\mathcal{F}}\}$. A família $\mathcal{F}$ é admissível. Considere a álgebra de Hopf $\mathbb{Z}[G]$ como $(U(\mathfrak{g})_{\mathbb{Z}})_{\mathcal{F}}$.

Por construção, $\mathbb{Z}[G]$ é uma $\mathbb{Z}$-álgebra, $U(\mathfrak{g})_{\mathbb{Z}}$-invariante, tal que $\mathbb{F}[G_{\mathbb{F}}] \simeq \mathbb{F} \otimes \mathbb{Z}[G]$ (cf. [Kos]). Por isso é possível definir a ação de $U(\mathfrak{g})_{\mathbb{F}}$ em $\mathbb{F}[G_{\mathbb{F}}]$ da seguinte forma natural: se $k\varphi = k \otimes \varphi \in U(\mathfrak{g})_{\mathbb{F}}$ e $af = a \otimes f \in \mathbb{F}[G_{\mathbb{F}}]$, então $(k\varphi)(af) = ak.\varphi(f)$.

Teorema 4.5.9. Sejam G um grupo algébrico semissimples sobre $\mathbb{K}$, $\mathfrak{g}$ a álgebra de Lie de G e $\mathbb{F}$ um corpo algebricamente fechado. Então $U(\mathfrak{g})_{\mathbb{F}} \simeq D(G_{\mathbb{F}})$.

Dem: Defina a função $\epsilon : U(\mathfrak{g})_{\mathbb{F}} \to \mathbb{F}[G_{\mathbb{F}}]^*$ da seguinte forma: $\epsilon(\varphi)(f) = \varphi(f)(e) \in \mathbb{F}$. Essa função é um morfismo injetor de álgebras de Hopf cuja imagem é $D(G_{\mathbb{F}})$. De fato:

(i) ϵ está bem definida pois os elementos da imagem são transformações lineares :

$$\begin{aligned}\epsilon(\varphi)(\lambda f_1 + f_2) &= \varphi(\lambda f_1 + f_2)(e)\\ &= (\lambda\varphi(f_1) + \varphi(f_2))(e)\\ &= \lambda\varphi(f_1)(e) + \varphi(f_2)(e)\\ &= \lambda\epsilon(\varphi)(f_1) + \epsilon(\varphi)(f_2).\end{aligned}$$

(ii) ϵ é linear :

$$\begin{aligned}\epsilon(\lambda\varphi + \psi)(f) &= (\lambda\varphi + \psi)(f)(e)\\ &= (\lambda\varphi(f) + \psi(f))(e)\\ &= \lambda\varphi(f)(e) + \psi(f)(e)\\ &= \lambda\epsilon(\varphi)(f) + \epsilon(\psi)(f)\\ &= (\lambda\epsilon(\varphi) + \epsilon(\psi))(f).\end{aligned}$$

(iii) ϵ é morfismo de álgebras :

$$\begin{aligned}\epsilon(\varphi\psi)(f) &= (\varphi\psi)(f)(e)\\ &= \left(\sum \varphi(f_1)\psi(f_2)\right)(e) \quad \text{(usando a comultiplicação)}\\ &= \sum \varphi(f_1)(e)\psi(f_2)(e)\\ &= \sum \epsilon(\varphi)(f_1)\epsilon(\psi)(f_2)\\ &= (\epsilon(\varphi)\epsilon(\psi))(f).\end{aligned}$$

(iv) ϵ é morfismo de coálgebras :

$$\begin{aligned}&\epsilon(\Delta(\varphi))(f_1, f_2) = (\Delta(\varphi))(f_1, f_2)(e) = \varphi(f_1 f_2)(e) \ e\\ &\Delta(\epsilon(\varphi))(f_1, f_2) = \epsilon(\varphi(f_1 f_2)) = \varphi(f_1 f_2)(e).\end{aligned}$$

(v) ϵ claramente preserva antípoda, portanto ϵ é morfismo de álgebras de Hopf.

(vi) ϵ é injetora :

Se $\epsilon(\varphi) = \epsilon(\psi)$, então para todo $f \in \mathbb{F}[G_{\mathbb{F}}]$, $\varphi(f)(e) = \psi(f)(e)$. Como φ e ψ são invariantes à esquerda, então $\varphi(f) = \psi(f)$. Logo $\varphi = \psi$.

(*vii*) Imagem de ϵ:

Se $\varphi \in U_m \setminus U_{m-1}$ então existem $\varphi_1, \ldots, \varphi_m \in U_1$, tais que $\varphi = \mu_U(\varphi_1, \ldots, \varphi_m)$. Portanto para cada $f \in \mathbb{F}[G_\mathbb{F}]$, $\varphi(f) = (\varphi_1 \otimes \ldots \otimes \varphi_m) \circ \Delta^m(f)$. Se $f \in I_e^{m+1}$ então, usando iteradamente a proposição 4.3.4, $\epsilon(\varphi)(f) = 0$. Logo $\epsilon(\varphi) \in D_m$.

Por outro lado, considere uma distribuição $d \in D_m$. Pelo isomorfismo da proposição 3.3.11, existe um único $\delta \in (\mathbb{K}[G]/I_e^{m+1})^*$ que corresponde a d. Considere agora a função $\tilde{\delta} : \mathbb{K}[G] \to \mathbb{K}[G]$ tal que $\tilde{\delta}(f)(g) = \delta(E_g^* f)$ para cada $f \in \mathbb{K}[G]$ e $g \in G$. Usando o isomorfismo descrito no teorema 4.2.5, existe um único $\varphi \in U_m$ que corresponde a $\tilde{\delta}$, para o qual φ, $\epsilon(\varphi) = d$.

Portanto $\epsilon : U(\mathfrak{g})_\mathbb{F} \to D(G_\mathbb{F})$ é um isomorfismo de álgebras de Hopf. □

4.6 Conclusão

Nessa seção, vamos expor alguns resultados (sem demonstrá-los) que motivam a dissertação e que são os passos mais naturais para continuação do estudo.

Sobre um corpo de característica zero, existe uma relação 1-1 entre as representações racionais de um grupo algébrico semissimples, conexo e simplesmente conexo e as representações de dimensão finita de sua álgebra de Lie. Existe também uma bijeção entre o conjunto de representações de dimensão finita de uma álgebra de Lie e de sua álgebra universal envelopante, por definição. Usando o teorema 4.5.9, concluímos que para cada representação racional de um grupo algébrico semissimples, conexo e simplesmente conexo, existe uma única representação de dimensão finita de sua álgebra de distribuições.

A pergunta natural é se existem tais relações também para o caso em que o corpo-base tem característica positiva. Nesse caso, a relação bijetiva entre o conjunto de representações racionais de um grupo algébrico semissimples, conexo e simplesmente conexo e o conjunto de representações de dimensão finita de sua álgebra de Lie continua válida. No artigo [Sul], Sullivan mostra que existe uma bijeção entre o conjunto das representações racionais de dimensão finita de um grupo algébrico conexo e simplesmente conexo e as representações da sua álgebra de distribuições. No artigo [Che2], Chevalley classifica os grupos de Chevalley, a saber, um grupo de Chevalley é um grupo algébrico conexo e semissimples e os grupos universais de Chevalley são os grupos algébricos semissimples, conexos e simplesmente conexos. Usando esse teorema e o teorema 4.5.9, concluímos que para cada representação de um grupo de Chevalley universal existe uma única representação de dimensão finita de sua álgebra de Lie, uma única representação de dimensão finita da sua álgebra de distribuições e consequentemente uma única representação de dimensão finita da hiperálgebra da sua álgebra de Lie.

Já que temos uma resposta para as perguntas anteriores, mostrando que a relação entre os grupos de Chevalley e suas álgebras de distribuição é tão estreita, gostaríamos de saber quais álgebras de Hopf são álgebras de distribuições de algum grupo algébrico e como reconstruir um grupo algébrico a partir de uma álgebra de distribuições.

Para isso, precisamos das seguintes definições, que se encontram em [Mon].

Definição 4.6.1.

(i) Seja C uma coálgebra. Uma subcoálgebra $C' \subseteq C$ é *simples* se não contém subcoálgebras próprias e não triviais.

(ii) Seja C uma coálgebra. O *coradical* C_0 de C é a soma de todas as subcoálgebras simples de C.

(iii) Uma coálgebra C é chamada de *conexa* se C_0 for unidimensional.

(iv) Seja H uma álgebra de Hopf. Defina o conjunto de *elementos primitivos de H* como $P(H) = \{x \in H \mid \Delta(x) = 1 \otimes x + x \otimes 1\}$.

Proposição 4.6.2. A álgebra de distribuições de um grupo algébrico sobre um corpo de característica zero é cocomutativa, finitamente gerada e conexa.

Dem: [Mon], cap.5. □

Usando a proposição anterior, vamos mostrar como reconstruir um grupo algébrico a partir de uma álgebra de Hopf cocomutativa, finitamente gerada e conexa sobre um corpo de característica zero.

Proposição 4.6.3. Seja H uma álgebra de Hopf cocomutativa e conexa, sobre um corpo $\mathbb{K}$ de característica zero. Então $H \simeq U(\mathfrak{g})$ para $\mathfrak{g} = P(H)$.

Dem: [Mon], p.79. □

Considere uma álgebra de Hopf cocomutativa, finitamente gerada e conexa sobre um corpo de característica zero. Considere $\mathfrak{g} = P(H)$. Pela proposição anterior, $H \simeq U(\mathfrak{g})$. Como H é finitamente gerada, $\mathfrak{g}$ é uma álgebra de Lie ([Mon], p.74) de dimensão finita (1.4.15) sobre um corpo de característica zero. Considere seu grupo de Chevalley universal $G_{\mathbb{K}}$. Usando o fato que $\mathbb{K}$ tem característica zero e o teorema 4.5.9, obtemos que $D(G_{\mathbb{K}}) \simeq H$. Por esse processo reconstruímos o grupo de Chevalley a partir da álgebra de Hopf.

No caso de característica positiva, o seguinte teorema contido em [Tak1] é importante:

Teorema 4.6.4 (de Takeuchi)**.** Seja $\mathbb{K}$ um corpo de característica positiva e G um grupo algébrico conexo sobre $\mathbb{K}$. G é simplesmente conexo se, e somente se, $D(G)^\circ \simeq \mathbb{K}[G]$.

Usando o teorema acima, obtemos que uma álgebra de Hopf é álgebra de distribuições de um grupo de Chevalley universal se, e somente se, sua álgebra dual finita for isomorfa a uma álgebra de funções regulares, ou seja, finitamente gerada e reduzida.

Definição 4.6.5. Seja H uma álgebra de Hopf e ε sua counidade. Defina H' como $H' = \{f \in H^\circ \mid \exists\ n \in \mathbb{N},\ f((\ker \varepsilon)^{n+1}) = 0\}$.

As álgebras de distribuições de grupos de Chevalley universais são álgebras de Hopf H que satisfazem a seguinte propriedade: $(H^\circ)' \simeq H$.

Além de nos prover da informação acima, o teorema de Takeuchi diz ainda como reconstruir o grupo algébrico a partir de sua álgebra de distribuições. A saber, considere uma tal álgebra de Hopf, cuja álgebra dual finita é isomorfa à uma álgebra de funções regulares, isto é, uma álgebra finitamente gerada e reduzida. Então usando a equivalência de categorias entre tais álgebras e variedades afins é possível reconstruir o grupo algébrico cuja álgebra de distribuições é a álgebra de Hopf inicial.

Do ponto de vista funtorial (como descrito nas seções 3.1.7 e 4.1), o teorema de Takeuchi nos permite explicitar o esquema de grupo que corresponde a uma álgebra de Hopf H satisfazendo $(H^\circ)' = H$, a saber, SpH°. Esse resultado nos incentiva a seguir estudando os funtores de esquemas de grupo como forma de entender alguns análogos aos grupos algébricos em dimensão infinita. Aliado ao fato acima, o incentivo também vem do fato de, por um lado, a teoria de variedades algébricas de dimensão infinita não ser bem desenvolvida e, por outro lado, a construção de análogos à hiperálgebras em dimensão infinita, a saber, as hiperálgebras de laços, admitirem construção mais simples. Nesse sentido, pretendemos estudar os funtores de esquemas de grupos da forma SpH°, onde H é uma hiperálgebra de laços.

Bibliografia

[Ana] A. Anan'in, Notas de aula de categorias e álgebra (co)homológica.

[Ati] M. Atiyah, I. MacDonald, Introduction to Commutative Algebra, Addison-Wesley (1969).

[CPS] E. Cline, B. Parshall, L. Scott, Cohomology, hyperalgebras, and representations, J. Algebra 63 (1980), 98-123.

[Che1] C. Chevalley, Certains schémas de groupes semissimples, Séminaire Bourbaki 13e année, 219 (1960/61). (1980), 98-123.

[Che2] C. Chevalley, Sur certains groupes simples, Tohoku Math. Jour. (1955), 14-66.

[Die] J. Dieudonnè, Sur les groupes de Lie algébriques sur un corps de caractéristique $p > 0$, Rend. Circ. Mat. Palermo 1 (1952), 380-402.

[Eis] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, GTM150 Springer (1999).

[Hab] W. J. Haboush, Central differential operators on split semi-simple groups over fields of positive characteristic, Lecture Notes in Mathematics, Séminaire d'Algèbre Paul Dubreil et Marie-Paule Malliavin, 795, Springer (1980).

[Har] R. Hartshorne, Algebraic Geometry, GTM52 Springer (1977).

[Hum1] J. Humphreys, Introduction to Lie algebras and representation theory, GTM9 Springer (1972).

[Hum2] J. Humphreys, Linear algebraic groups, GMT21 Springer (1981).

[Jac] N. Jacobson, Lie algebras, Interscience Tracts on Pure and Applied Mathematics, no. 10. Interscience Publishers, New York (1962).

[Jan] J. Jantzen, Representation of algebraic groups, Mathematical Surveys and Monographs **107**, AMS (2003).

[Kos] B. Kostant, Groups over $\mathbb{Z}$, Proc. Symposia in Pure Math., **9** (1966), 90-98.

[Mac] S. MacLane, Categories for the working mathematcian, GTM5 Springer (1971).

[Mon] S. Montgomery, Hopf algebras and their actions on rings, CBMS Regional Conference Series in Mathematics **82**, AMS (1993).

[Ree] R. Ree, On some simple groups defined by C. Chevalley, Trans. Amer. Math. Soc., **84** (1957), 392-400.

[Ste] R.G. Steinberg, Lectures on Chevalley groups , Yale Univ. Press (1968).

[Sul] W. Sullivan, Simply connected groups, the hyperalgebra, and Verma's conjecture, American Journal of Mathematics, Vol. 100, No. 5, (Oct., 1978).

[Tak1] M. Takeuchi, On coverings and hyperalgebras of affine algebraic groups, Trans. Amer. Math. Soc. 211 (1975), 249-275.

[Tak2] M. Takeuchi, Generators and relations for the hyperalgebras of reductive groups, J. Algebra, **85**, 197-212 (1983).

[Yan] H. Yanagihara, Theory of Hopf algebras attached to group schemes, Lecture notes in mathematics, 614, Springer (1977).

Índice