Estruturas livres em anéis de divisão

Renato Fehlberg Júnior

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura:

Estruturas livres em anéis de divisão

Renato Fehlberg Júnior

Orientador: **Prof. Dr. Eduardo Tengan**

Coorientador: **Prof. Dr. Daniel Levcovitz**

Tese apresentada ao Instituto de Ciências Matemáticas e de Computação - ICMC-USP, como parte dos requisitos para obtenção do título de Doutor em Ciências - Matemática . *VERSÃO REVISADA*

USP – São Carlos
Junho de 2013

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados fornecidos pelo(a) autor(a)

Fehlberg Júnior, Renato
F296e Estruturas livres em anéis de divisão / Renato Fehlberg Júnior; orientador Eduardo Tengan; co-orientador Daniel Levcovitz. -- São Carlos, 2013.
66 p.

Tese (Doutorado - Programa de Pós-Graduação em Matemática) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2013.

1. Álgebra de divisão. 2. Álgebras livres. I. Tengan, Eduardo, orient. II. Levcovitz, Daniel, co-orient. III. Título.

It's a dangerous business ... going out of your door. You step into the road, and if you don't keep your feet, there's no knowing where you might be swept off to.
The Lord of the Rings - The fellowship of the ring

Agradecimentos

Primeiramente, agradeço a Deus por mais essa benção em minha vida, por cada vez que aprendi com os erros e pelos momentos de alegria e sucesso. Obrigado Senhor!

Aos meus orientadores, Daniel e Eduardo, por todo conhecimento adquirido, pela experiência acadêmica e pela amizade. De modo especial, agradeço ao Eduardo pelas conversas, ensinamentos e por me conduzir com competência e sabedoria durante essa caminhada. Sempre tinha um bom conselho e um contra-exemplo para me dar. Muito obrigado!

Aos meu familiares, pelos momentos que passamos juntos, por cada sorriso e palavra de motivação. Um agradecimento muito especial aos meus pais, Wanda e Renato, pelo amor e dedicação incondicional não afetados pela distância ou pelo tempo. Agradeço também a Maria e ao Geraldo pelo carinho com que me receberam em sua família.

À minha amada esposa, por ter tornado cada dia dessa jornada mais especial. Obrigado por entrar em minha vida e não querer mais sair. Te amo muito!

Sem dúvida, nenhuma jornada seria completa sem a presença de amigos. Uns chegam, outros vão, mas aqueles que realmente são importantes nunca deixam nossas vidas, seja por uma boa lembrança ou pelo fruto de suas ações. Aos meus amigos de Itaguaçu, que mesmo distantes mostraram como uma amizade pode ser forte e duradoura; são muitos, mas cada um sabe em seu coração o quanto são especiais em minha vida. Também tem aquelas amizadas que surgiram no meio acadêmico; agradeço a todos pelos bons momentos juntos. Em especial, ao Vinícius, Paulo, Northon e a Carol, pelas boas conversas e os momentos impressindíveis em minha vida, assim como a amizade. Ao grupo de RPG de São Carlos, que se tornaram grandes amigos e por terem contribuido em mais essa quest.

Por fim, agradeço à FAPESP pelo apoio financeiro.

Resumo

A conjectura de Makar-Limanov afirma que se um anel de divisão D é finitamente gerado e de dimensão infinita sobre seu centro k, então D contém uma k-subálgebra livre de posto 2. Neste trabalho, investigaremos a existência de tais estruturas no anel de divisão de frações do anel de polinômios skew $L[t;\sigma]$, onde t é uma variável e σ é um k-automorfismo de L. Mais especificamente, assumindo o que chamamos de Hipótese do Delta 3.3.1, provaremos esse resultado para L/k uma extensão de corpos, mesmo quando L não é finitamente gerado sobre k. Finalmente, provaremos a Hipótese do Delta e a conjectura, quando L é o corpo de funções de uma variedade abeliana ou o corpo de funções do espaço projetivo n-dimensional.

Abstract

Makar-Limanov's conjecture states that if a division ring D is finitely generated and infinite dimensional over its center k then D contains a free k-subalgebra of rank 2. In this work, we will investigate the existence of such structures in the division ring of fractions of the skew polynomial ring $L[t;\sigma]$, where t is a variable and σ is an k-automorphism of L. More specifically, assuming what we called Delta's Hipothesis 3.3.1, we prove this result for L/k a field extension, even when L isn't finitely generated over k. Finally, we prove Delta's Hipothesis and the conjecture when either L is the function field of an abelian variety or the function field of the n-dimensional projective space.

Sumário

Introdução **xi**

1 Pré-requisitos **1**
1.1 Domínios de Ore 2
1.2 Variedades 6
1.3 Geometricamente irredutível, reduzido e integral 10
1.3.1 Resultados gerais sobre corpos 13
1.3.2 Álgebras geometricamente reduzidas 18
1.3.3 Álgebras geometricamente irredutíveis e integrais 22
1.3.4 Variedades geometricamente integrais 30

2 A conjectura de Makar-Limanov **37**
2.1 Resultados conhecidos 37
2.2 Discussão e contra-exemplos I 41
2.3 Discussão e contra-exemplos II 43

3 Resultados gerais **45**
3.1 Setup 45
3.2 Lemas 47
3.3 O teorema 51
3.4 Conjectura GA 57

4 Hipótese do Delta **59**
4.1 Variedades Abelianas 60
4.2 Espaço Projetivo 61

Referências Bibliográficas **66**

Introdução

Anéis de divisão, álgebras de divisão ou ainda corpos skew (que são corpos onde os elementos, na multiplicação, não necessariamente comutam), sempre foram objetos que intrigaram muitos matemáticos por sua complexidade. O primeiro exemplo desse tipo de estrutura, os quatérnios reais, foi obtido por W.R. Hamilton em 1843 na tentativa de generalizar a representação por pontos no plano dos números complexos. Esse também foi um importante exemplo de álgebra de divisão de dimensão finita sobre $\mathbb{R}$, que na verdade, é o único exemplo sobre $\mathbb{R}$ (sobre outros corpos, essa questão é muito mais complicada). Mais de 100 anos se passaram e pouco foi feito sobre anéis de divisão. A teoria se desenvolveu na direção de álgebras de quatérnios generalizadas, produtos cruzados, firs (free ideal rings), dentre outros.

Em 1971 J. Tits em [Tit72] provou que em característica 0 um grupo linear ou tem um subgrupo livre não-abeliano ou possui um subgrupo solúvel de índice finito (todo subgrupo finitamente gerado de um grupo de matrizes ou contém um subgrupo livre não-cíclico ou é solúvel-por-finito). Esse resultado ficou conhecido como a *Alternativa de Tits*. Algum tempo depois, S. Bachmuth, na tentativa de generalizar o resultado de Tits, questionou se era possível trocar "corpo" por "anel de divisão" na hipótese do teorema. Em 1977, A.I. Lichtman em [Lic77] respondeu essa questão dando um contra-exemplo, mostrando que mesmo no caso de matrizes 1×1 sobre um anel de divisão, ou seja, o próprio anel de divisão, o problema proposto por Bachmuth era falso. O contra-exemplo consistia em mostrar que para certo corpo skew D, o grupo multiplicativo D^* contém um subgrupo finitamente gerado que satisfaz uma identidade não-trivial e não tem subgrupo normal solúvel de índice finito. Nesse mesmo artigo, Lichtman propôs a seguinte conjectura, que foi um grande passo no estudo da estrutura das álgebras de divisão:

Conjectura G (Lichtman)**.** *O grupo multiplicativo $D^\times$ de um anel de divisão D contém um grupo livre não cíclico.*

Poucos anos depois alguns resultados particulares dessa conjectura já tinham sido provados pelo próprio Lichtman em [Lic78] e [Lic82]. Isso despertou o interesse de outros matemáticos no estudo da estrutura das álgebras de divisão na direção da conjectura de Lichtman.

Em 1983, L. Makar-Limanov apresentou um primeiro resultado sobre a existência de subálgebras livres em anéis de divisão, que na verdade, foi um problema inicialmente proposto pelo matemático L. Small. Em [ML83], Makar-Limanov provou que no anel de divisão de frações da álgebra de Weyl $D_1 = \mathrm{Frac}(k[x,y]/(yx-xy-1))$, com $\mathrm{char}k = 0$, podemos encontrar subálgebras livres de posto 2. No ano seguinte, em 1984, Makar-Limanov propôs em [ML84a] a seguinte:

Conjectura A (Makar-Limanov)**.** *Seja D um corpo skew com centro k. Se D é finitamente gerado e de dimensão infinita sobre k então D contém subálgebras livres de posto* 2*.*

Lembre que o centro de um anel de divisão D é o conjunto $Z(D) \stackrel{def}{=} \{a \in D; ab = ba \ \forall\, b \in D\}$. O centro de D é necessariamente um corpo (basta notar que se $xy = yx$, para $x \in D$ e $0 \neq y \in Z(D)$, obtemos $y^{-1}x^{-1} = x^{-1}y^{-1}$ e assim $y^{-1} \in Z(D)$).

Desde que Makar-Limanov conjecturou sobre a existência de estruturas livres em certos anéis de divisão, matemáticos têm provado casos particulares dessa conjectura, que parece estar longe de uma solução geral. Nesse sentido, Makar-Limanov diz o seguinte em [ML84a]: "*...is very difficult in such generality because it contains as very special case the Kurosh conjecture. Nevertheless one can try to investigate some concrete skew fields where it is also quite a challenge*". Um dos poucos resultados gerais, com relação a existência de estruturas livres e ao problema do cancelamento, são devido a Z. Reichstein e A. Smoktunowicz. Em [Rei96], Reichstein provou que se *A é uma álgebra sobre um corpo k não-enumerável e se $F \otimes_k A$ contém uma álgebra livre de posto* 2*, então A também contém*, onde F/k é uma extensão de corpos. Porém, em [Smo09], Smoktunowicz provou que se retirarmos a hipótese de que k é não-enumerável, então é possível encontrar uma k-álgebra que contradiz o teorema de Reichstein. É importante observar que a álgebra encontrada por Smoktunowicz é nil e portanto o caso de corpos skew ainda está em aberto. Ambos resultados, dentre outros, serão descritos e discutidos com mais detalhes no Capítulo Dois.

Vale ressaltar que encontrar a solução da conjectura de Makar-Limanov, nos permitiria responder o *Problema de Kurosh* para anéis de divisão. O *Problema de Kurosh* consistia na seguinte afirmação: ***uma álgebra finitamente gerada e algébrica sobre o seu corpo base k é de dimensão finita sobre k***. Depois, o problema foi reformulado da seguinte forma: ***em uma álgebra finitamente gerada A sobre um***

corpo** k**, se todo elemento é nilpotente, então** A **é nilpotente? Esse problema era o equivalente para álgebras de uma conjectura ainda mais antiga. Em 1902, W. Burnside propôs o seguinte problema: ***seja** G **um grupo de torção finitamente gerado. Então,** G **é finito?*** Esse problema ficou conhecido como a *Conjectura de Burnside* (General Burnside Problem). Porém, em 1964, Golod e Shafarevich apresentaram um contra-exemplo para essa conjectura e para o Problema de Kurosh: em "*On nil algebras and approximable groups*" e "*On towers of class fields*", eles construíram uma álgebra nil de dimensão infinita gerada por 3 elementos e um grupo infinito de torção gerado também por 3 elementos. Porém, o Problema de Kurosh para anéis de divisão ainda continua em aberto:

Problema de Kurosh . *Se D é um anel de divisão finitamente gerado e algébrico sobre seu centro k, então D é de dimensão finita sobre k.*

Outro aspecto interessante no estudo de estruturas livres em anéis de divisão, é a seguinte conjectura que fala sobre a existência de álgebras de grupo em anéis de divisão. Uma álgebra de grupo $k[G]$, onde k é um corpo e G um grupo, é definida como o conjunto das somas finitas formais $\sum_{g\in G} a_g g$ com operações definidas do modo usual (um espaço vetorial sobre k). Temos:

Conjectura GA. *Seja D um corpo skew com centro k. Se D é finitamente gerado e de dimensão infinita sobre k então D contém uma álgebra de grupo livre sobre k.*

Portanto, a conjectura GA implica nas conjecturas de Lichtman e Makar-Limanov, o que indica o grau de dificuldade em se buscar a solução geral ou mesmo uma solução parcial para essa conjectura. Veremos no Capítulo Dois mais relações entre essas três conjecturas (também conhecidas como *conjecturas FOFO* (full of free objets)).

Nesse trabalho, estamos interessados em estudar a conjectura de Makar-Limanov quando o corpo skew D é a álgebra de divisão de frações de um anel de polinômios skew $L[t;\sigma]$ (anel de polinômios em t não-comutativo), onde t é uma variável e σ é um k-automorfismo de L, sendo L/k uma extensão de corpos. Provar a conjectura de Makar-Limanov nesse caso, é provar que existe uma cópia homomórfica da álgebra livre $k\langle x, y\rangle$ sobre dois geradores x, y em D, ou seja, vamos exibir dois elementos em D que são as imagens de x, y. Além disso, aplicando um resultado de Lichtman (ver Seção 3.4) obteremos um caso particular da conjectura GA. Nesse sentido, generalizamos os resultados de [GT09] e [Lor86]. Enfatizamos que esses dois resultados não serão contemplados neste trabalho como casos particulares por causa do método usado.

Dois trabalhos recentes e que devem ser destacados são devido a J.P. Bell e D. Rogalski, nos artigos [BRa] e [BRb]. No primeiro, eles provam que se A é um domínio

noetheriano que é contavelmente gerado sobre um corpo algebricamente fechado não-enumerável k de característica zero, então ou a algebra de divisão de frações de A contém uma álgebra livre de posto 2 ou ela é algébrica à esquerda sobre todo subcorpo maximal. No segundo, eles provam que $K(x;\sigma)$ contém uma álgebra livre de posto 2, onde K/k é extensão de corpos, onde ou k é não-enumerável ou σ é induzido por um automorfismo de uma variedade quase-projetiva. Neste ponto, o presente trabalho se diferencia pelas técnicas usadas, onde diferentes geradores são encontrados e por tratar a conjectura sob outro ponto de vista. Além disso, os primeiros resultados são apresentados de uma forma bem geral, com hipóteses bem fracas sobre o corpo base. Espera-se que as técnicas aqui apresentadas sirvam de suporte para futuras generalizações, principalmente para o caso em que k é enumerável, onde tem-se obtido poucos resultados.

O presente trabalho está dividido em quatro partes. No primeiro capítulo, serão apresentados os pré-requisitos para a leitura deste texto. Definiremos os principais objetos, como o anel de polinômios skew $L[t;\sigma]$ e seu anel de divisão de frações $\mathrm{Frac}(L[t;\sigma]) = L(t;\sigma)$. Para isso, faremos um pouco da teoria de álgebra não-comutativa. Além disso, mostraremos alguns resultados sobre esquemas e variedades projetivas, como o famoso Teorema de Bertini 1.2.11. Finalizaremos o capítulo com uma seção inteiramente dedicada ao estudo de álgebras e esquemas geometricamente integrais, onde apresentaremos detalhadamente os resultados e suas equivalências. No segundo capítulo, será feita uma breve abordagem sobre os resultados já conhecidos sobre a conjectura de Makar-Limanov, destacando-se os principais resultados de cada artigo. Além disso, serão dados alguns contra-exemplos e justificativas, mostrando que certas hipóteses não podem ser enfraquecidas e outras não afetam a generalidade dos resultados. No capítulo três, sujeito ao que chamamos de *Hipótese do Delta* 3.3.1, provaremos o seguinte resultado

Teorema 0.0.1. *Sejam k um corpo, L/k uma extensão própria de corpos tal que k é algebricamente fechado em L e σ um k-automorfismo de L tal que $L^{\langle\sigma\rangle} = k$. Seja $f \in A \setminus k$ para alguma k-subálgebra A de L no qual vale a Hipótese do Delta 3.3.1. Então, os elementos f e $t(1-t)^{-1}f$ geram uma álgebra livre sobre k em $D = L(t;\sigma)$.*

Além disso, obteremos como corolário desse teorema, um caso particular da conjectura GA. No último capítulo, provaremos casos particulares da *Hipótese do Delta*: quando L é o corpo de funções de uma variedade abeliana ou L é o corpo de funções do espaço projetivo.

✓

Capítulo

1

Pré-requisitos

Aqui apresentaremos os resultados básicos que serão usados ao longo deste trabalho. Na primeira seção, definiremos o anel de polinômios skew, que é um domínio não-comutativo e um dos principais objetos que estudaremos. No caso de um domínio comutativo podemos definir sem muita dificuldade um corpo de frações. Quando o domínio é não-comutativo, precisaremos de condições especiais para definirmos um anel de divisão de frações (à direita ou à esquerda), por analogia ao caso comutativo. Na segunda seção, faremos uma breve apresentação sobre variedades algébricas e projetivas. A terceira seção será a mais importante deste capítulo. Nela, falaremos sobre álgebras e variedades que mantêm certas propriedades após uma mudança de base. A notação será padrão durante todo o texto a menos de algumas exceções.

Notação 1.0.2. Ao longo do texto sempre teremos:

1. k um corpo (comutativo); ou seja, sempre que nos referirmos a um corpo, estamos falando no sentido comutativo;

2. $\overline{k}$ é o fecho algébrico de k; k^s é o fecho separável de k; $k^{1/p}$ é a menor extensão de k que contém todas as p-ésimas raízes de cada elemento de k; $k^{p^{-\infty}}$ é o fecho perfeito de k. Necessariamente quando falarmos de $\overline{k}$ estaremos fazendo uma escolha de um fecho algébrico de k e consequentemente teremos k^s e $k^{p^{-\infty}}$ determinados. Nessas condições temos necessariamente que $k^{1/p} \hookrightarrow k^{p^{-\infty}} \hookrightarrow \overline{k}$

3. L uma extensão de corpos de k, que sempre será entendida como L *uma extensão de corpos de* k *com* $L \neq k$.

1.1 Domínios de Ore

Nesta seção definiremos e provaremos resultados de álgebra não-comutativa. Apesar de alguns desses resultados serem parecidos com o caso comutativo, devem-se tomar certos cuidados. As principais referências são: [Coh77], [Coh06], [GW89] e [Lam01].

Como foi dito anteriormente, gostaríamos de definir, de modo análogo ao caso comutativo, um "corpo de frações". No caso não-comutativo isso é um pouco mais complicado e obteremos um anel de divisão de frações à direita (resp. à esquerda). Para isso, precisaremos impor mais uma condição sobre o domínio, conhecida como *condição de Ore* à direita (resp. à esquerda).

Definição 1.1.1. *Sejam D um domínio e S um conjunto multiplicativo, ou seja, um subconjunto de D tal que $1_D \in S$ e se $a, b \in S$ então $ab \in S$. Dizemos que S é um conjunto de Ore à direita (resp. à esquerda) se para todo par $x \in D$ e $y \in S$ temos $xS \cap yD \neq \emptyset$ (resp. $Sx \cap Dy \neq \emptyset$). Essa é a condição de Ore à direita (resp. à esquerda). O domínio D é de Ore à direita (resp. à esquerda) se $S = D \setminus \{0\}$ é Ore à direita (resp. à esquerda). Quando um domínio é de Ore à direita e à esquerda, ele é chamado simplesmente domínio de Ore.*

Exemplo 1.1.2. Exemplo de domínio não-comutativo que não satisfaz a condição de Ore à direita. Seja $R = k\langle x, y\rangle$ a álgebra associativa livre de posto 2 sobre k. Seja $S = R \setminus \{0\}$. Temos que S é um conjunto multiplicativo que não é Ore à direita. De fato, tome os elementos $x, y \in S$ e note que $xS \cap yR = \emptyset$, pois caso contrário isso implicaria na comutatividade entre x e y.

Como no caso comutativo, temos uma definição de módulo e anel noetheriano:

Definição 1.1.3. *Seja A um anel. Um A-módulo à direita M (resp. à esquerda) é noetheriano à direita (resp. à esquerda) se ocorre uma, e portanto todas, as seguintes condições equivalentes:*

1. *Toda cadeia ascendente própria de A-submódulos à direita (resp. à esquerda) é estacionária.*

2. *Toda família não vazia de A-submódulos à direita (resp. à esquerda) tem um elemento maximal.*

3. *Todo A-submódulo à direita (resp. à esquerda) é finitamente gerado.*

Desse modo, temos a:

Definição 1.1.4. *Um anel R é noetheriano à direita (resp. à esquerda) se R visto como R-módulo à direita (resp. à esquerda) é noetheriano à direita (resp. à esquerda). Se ambos ocorrem, R é um anel noetheriano.*

Domínios noetherianos são importantes pois:

Proposição 1.1.5. *Qualquer domínio noetheriano à direita (resp. à esquerda) é Ore à direita (resp. à esquerda). Além disso, todo domínio noetheriano é um domínio de Ore.*

Demonstração: Seja D um domínio noetheriano à direita e sejam $a, b \in D \setminus \{0\}$. Queremos mostrar que $aD \cap bD \neq \{0\}$. Como D é noetheriano à direita, temos que $\sum_0^\infty a^i bD$ é finitamente gerado. Portanto, existem $n > 0$ e $c_0, \ldots, c_{n-1} \in D$ tais que

$$a^n b = bc_0 + abc_1 + \ldots + a^{n-1}bc_{n-1}.$$

Como $a^n b \neq 0$, os c_i's não são todos nulos. Seja c_k o primeiro coeficiente não nulo. Cancelando a^k em ambos os lados obtemos

$$a^{n-k}b = bc_k + abc_{k+1} + \ldots + a^{n-k-1}bc_{n-1}.$$

Portanto, $bc_k \in aD$, ou seja, $aD \cap bD \neq \{0\}$. A prova para o caso à esquerda é análogo. ■

Queremos ainda saber se um domínio de Ore possui anel de divisão de frações no sentido clássico. A condição de Ore foi criada para isso, como veremos a seguir.

Definição 1.1.6. *Um anel de divisão de frações à direita (resp. à esquerda) para um domínio D é um anel de divisão, denotado por* $\mathrm{Frac}(D)$*, tal que D é subanel de* $\mathrm{Frac}(D)$ *e todo elemento de* $\mathrm{Frac}(D)$ *é da forma $ab^{-1} = a/b$ (resp. $b^{-1}a = a/b$), com $a \in D$ e $b \in D \setminus \{0\}$*

A prova de que todo domínio de Ore à direita (resp. à esquerda) possui um anel de divisão de frações à direita (resp. à esquerda) é um caso particular da localização à direita (resp. à esquerda) no caso não-comutativo.

Definição 1.1.7 (Localização à direita)**.** *Seja D um domínio e seja S um conjunto (multiplicativo) de Ore à direita. A localização à direita de D em S, denotada por D_S, é feita da seguinte forma: sobre $D \times S$ defina uma relação de equivalência dizendo que $(a, b) \sim (a', b')$ se, e somente se, existem $t, t' \in S$ tais que $at = a't'$ e $bt = b't'$. Portanto,*

$$D_S = (D \times S)/\sim$$

e denote a classe de um par (a, b) convenientemente por a/b. Antes de definir as operações de soma e produto sobre D_S, precisamos saber como igualar os denominadores. Procedemos assim: se $a/b, a'/b' \in D_S$ então existem $t, t' \in S$ tal que $bt = b't'$ e portanto, escrevemos $a/b = at/bt$ e $a'/b' = a't'/b't'$, ambas expressões com o mesmo denominador. Então, definimos a soma por

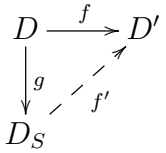
$$a/b + a'/b' = at/bt + a't'/b't' = (at + a't')/bt.$$

Para a multiplicação, tome $d \in D$ e $s \in S$ tais que $a's = bd$ (pois S é conjunto de Ore à direita) e temos

$$(a/b)(a'/b') = ab^{-1}a'(b')^{-1} = ads^{-1}(b')^{-1} = ad(b's)^{-1} = ad/b's.$$

A localização à direita satisfaz a seguinte

Propriedade Universal: dado um morfismo qualquer $f : D \to D'$, tal que todo elemento de $f(D)$ é inversível em D' então existe uma única $f' : D_S \to D'$ tal que $f' \circ g = f$, onde $g : D \to D_S$ é dado por $d \mapsto d/1$.



A localicação à esquerda é feita de maneira análoga e também temos uma propriedade universal. Finalmente temos o seguinte resultado:

Teorema 1.1.8. *Se D é um domínio de Ore à direita (resp. à esquerda) então D possui um anel de divisão de frações à direita (resp. à esquerda).*

Demonstração: Tome $S = D\backslash\{0\}$ (conjunto de Ore à direita). Fazendo a localização à direita de D em S obtemos $\mathrm{Frac}(D) \stackrel{def}{=} D_S$, que é um anel, onde $0/1$ é o zero e $1/1$ é a unidade do produto. A aplicação $d \mapsto d/1$ nos dá um homomorfismo injetor de anéis de D para $\mathrm{Frac}(D)$. De fato, é claro que essa aplicação é um homomorfismo de anéis. Para ver a injetividade, suponha que $d/1 = 0/1$, ou seja, $(d, 1) \sim (0, 1)$. Por definição, existem $t, t' \in S$ tais que $dt = 0t' = 0$. Como D é domínio, obtemos $d = 0$. Portanto, podemos olhar D como subanel de $\mathrm{Frac}(D)$. Além disso, $\mathrm{Frac}(D)$ é um anel de divisão: se a/b é diferente de zero em $\mathrm{Frac}(D)$ então $a, b \in S$ e $b/a \in \mathrm{Frac}(D)$. Claramente temos $(a/b) \cdot (b/a) = 1/1$ e $(b/a) \cdot (a/b) = 1/1$. Isso encerra a prova. O caso em que D é domínio de Ore à esquerda é demonstrado de maneira análoga.

■

Como no caso comutativo, temos:

Proposição 1.1.9. *O anel de divisão de frações à direita (resp. à esquerda) de um domínio de Ore à direita D (resp. à esquerda) é único a menos de isomorfismo.*

Demonstração: Escreva $S = D \setminus \{0\}$ e suponha que K é outro anel de divisão de frações de D. Temos mergulhos $g : D \to K$ e $h : D \to \mathrm{Frac}(D)$. Afirmamos que o homomorfismo

$$f : \mathrm{Frac}(D) \to K$$

dado por $a/b \mapsto g(a)/g(b)$ é injetivo. De fato, se d/s está no núcleo de f então $f(d/s) = g(d)/g(s) = 0$. Portanto, $g(d) = 0$ e consequentemente $d = 0$ pois g é injetora. Mas, $f(h(D)) \subset f(\mathrm{Frac}(D)) \subset K$ como subconjunto e portanto são iguais. Desse modo, f é isomorfismo como queríamos.

■

Como haviamos dito, estamos interessados no anel de polinômios skew. Veremos que ele é um domínio noetheriano e desse modo possui um anel de divisão de frações.

Definição 1.1.10 (Anel de polinômios skew)**.** *Sejam R um anel, σ um automorfismo de R e x uma indeterminada. Para cada $a \in R$ colocamos $xa = \sigma(a)x$. Desse modo, temos o anel de polinômios skew $R[x;\sigma]$, que é um anel de polinômios na indeterminada x com coeficientes em R não comutativo.*

Observação 1.1.11. O anel de séries de potência skew $R[[x;\sigma]]$ e o anel de séries de Laurent skew $R((x;\sigma))$ são definidos da mesma maneira (para as potências negativas, precisamos aplicar a condição de Ore de modo análogo ao feito na demonstração do Lema 1.1.14).

Proposição 1.1.12. *Seja k um corpo. Então, $k[x;\sigma]$ é um domínio noetheriano.*

Esse resultado é um caso particular do Teorema da Base de Hilbert para anéis de polinômios skew:

Teorema 1.1.13 ([GW89] pág.13 teor.1.12)**.** *Seja R um anel e σ um automorfismo de R. Se R é noetheriano à direita (resp. à esquerda) então $R[x;\sigma]$ é noetheriano à direita (resp. à esquerda)*

Como $k[x;\sigma]$ é domínio noetheriano (à direita e esquerda, pois k é corpo), então ele é um domínio de Ore e portanto possui anel de divisão de frações $\mathrm{Frac}(k[x;\sigma]) \stackrel{def}{=} k(x;\sigma)$ que é exatamente a localização à direita (ou à esquerda) de $k[x;\sigma]$ em $S = k[x;\sigma] \setminus \{0\}$.

Finalizamos com o seguinte

Lema 1.1.14. *Seja k um corpo e σ um automorfismo de k de ordem infinita. Então, $Z(k((x;\sigma))) = k^{\langle\sigma\rangle}$, onde $k^{\langle\sigma\rangle}$ são os elementos de k fixos por σ. Em particular, $Z(k(x;\sigma)) = k^{\langle\sigma\rangle}$.*

Demonstração: Note que se $a \in k^{\langle\sigma\rangle}$, então $x^n a = \sigma^n(a)x^n = ax^n$ para todo $n \in \mathbb{Z}$ (quando n é negativo, existem $d, s \in k[x;\sigma]$ não nulos com $as = x^{-n}d$ e assim $x^n a = ds^{-1}$. Daí, tomamos $s = x^{-n}$ e $d = \sigma^n(a)$ e obtemos o resultado). Se $f = \sum_{i\geq n} a_i x^i \in k((x;\sigma))$ então

$$fa = (\sum_{i\geq n} a_i x^i)a = \sum_{i\geq n} a_i \sigma^i(a)x^i = \sum_{i\geq n} a_i a x^i = af.$$

Para a outra inclusão, seja $f = \sum_{i\geq n} a_i x^i \in Z(k((x;\sigma)))$ e tome $x \in k((x;\sigma))$. Temos que

$$xf = x\sum_{i\geq n} a_i x^i = \sum_{i\geq n} x a_i x^i = (\sum_{i\geq n} \sigma(a_i)x^i)x.$$

Mas, $xf = fx$ e assim $\sigma(a_i) = a_i$ para todo i, ou seja, $a_i \in k^{\langle\sigma\rangle}$ para todo i. Agora, seja $a \in k$. Temos $fa = \sum_{i\geq n} a_i x^i a = \sum_{i\geq n} a_i \sigma^i(a)x^i = af$. Como σ tem ordem infinita, segue que $a_i = 0$ exceto para $i = 0$, pois caso contrário, para todo i tal que $a_i \neq 0$ teríamos $\sigma^i(a) = a$. Portanto, $f \in k^{\langle\sigma\rangle}$.

Para finalizar, note que $k^{\langle\sigma\rangle} \subset Z(k(x;\sigma)) \subset Z(k((x;\sigma))) = k^{\langle\sigma\rangle}$. A primeira inclusão é feita da seguinte forma: seja $a \in k^{\langle\sigma\rangle}$. A comutatividade com polinômios decorre do caso anterior. Agora, se $f/g \in k(x;\sigma)$ então $a(f/g) = afg^{-1} = fag^{-1}$. Por outro lado, $fg^{-1}a = fds^{-1}$, para $d, s \in k[x;\sigma] \setminus \{0\}$ tais que $as = gd$. Como $as = sa$, escolho $s = g$ e $d = a$, obtendo $fg^{-1}a = fag^{-1}$, ou seja, $a \in Z(k(x;\sigma))$. Para a segunda inclusão, basta notar que os elementos da forma x^n, para $n \in \mathbb{Z}$, estão em $k(x;\sigma)$, ou seja, se $f/g \in Z(k(x;\sigma))$, então f/g trivialmente comuta com os elementos de $k((x;\sigma))$.

■

1.2 Variedades

No Capítulo Três, L/k será apenas uma extensão de corpos com algumas propriedades. Porém, no Capítulo Quatro, L será visto como o corpo de funções de uma variedade projetiva, que é um esquema com certas propriedades. Por isso, precisaremos da noção de esquemas e alguns resultados. Como esse assunto é um tanto quanto extenso, deixaremos apenas as referências. Recomendamos a leitura de [Har77] cap.II e [Liu02] cap.2 e 3, onde podem ser encontradas a definição de esquemas, construção de esquemas afins e de seu feixe estrutural, além de muitas de suas propriedades. Nesta seção, apresentaremos apenas algumas definições e as principais propriedades das variedades projetivas que usaremos, além do enunciado de alguns resultados clássicos.

Começamos com uma definição

Definição 1.2.1. *Seja $(X, \mathcal{O}_X)$ (ou simplesmente X) um esquema.*

- *X é reduzido se $\forall$ aberto afim $U \subset X$, o anel $\mathcal{O}_X(U)$ é reduzido (ou seja, 0 é o único nilpotente de $\mathcal{O}_X(U)$).*
- *X é irredutível se o espaço topológico X é irredutível.*
- *X integral significa reduzido e irredutível.*

Um critério útil para saber quando um esquema X é integral é o seguinte:

Teorema 1.2.2 ([Liu02] pág.65)**.** *Seja X um esquema. X é integral se, e somente se, $\mathcal{O}_X(U)$ é um domínio integral para todo aberto afim $U \subset X$.*

Muitos dos resultados que veremos na próxima seção serão válidos para esquemas, porém estaremos interessados mais especificamente em variedades algébricas. Temos a seguinte definição:

Definição 1.2.3. *Seja k um corpo.*

1. *Uma variedade algébrica sobre k é um esquema separado de tipo finito sobre k.*
2. *Uma variedade projetiva X sobre k é um esquema separado de tipo finito tal que o morfismo estrutural $\pi : X \to \mathrm{Spec}(k)$ é projetivo (i.e., π se fatora em uma imersão fechada $i : X \to \mathbb{P}^n_k$, para algum n, e uma projeção $\mathbb{P}^n_k \to \mathrm{Spec}(k)$).*

Exemplo 1.2.4.
1. $X = \mathrm{Spec}\,\mathbb{C}[x, y]$ é uma variedade algébrica (afim) sobre $\mathrm{Spec}(\mathbb{C})$.
2. A reta projetiva $\mathbb{P}^1_{\mathbb{C}}$ é uma variedade que não é afim. De fato, $\mathbb{P}^1_{\mathbb{C}}$ é a colagem de duas variedades afins, a dizer, $\mathrm{Spec}(\mathbb{C}[t])$ e $\mathrm{Spec}(\mathbb{C}[1/t])$ (para mais detalhes sobre colagem ver [Liu02] pág.49).

As duas variedades projetivas que veremos no Capítulo Quatro serão o espaço projetivo e a variedade abeliana. Vejamos suas definições e algumas de suas propriedades.

O espaço projetivo n-dimensional $\mathbb{P}^n_k$ é definido como o conjunto das classes de equivalência de $(n+1)$-uplas $(a_0, \ldots, a_n) \in k^{n+1} \setminus \{0\}$ sob a relação de equivalência: $(a_i) \sim (\lambda a_i)$ para todo $\lambda \in k^*$. Como esquema, temos as seguintes construções: por colagem de esquemas afins ([Liu02] pág. 50) ou direto como Proj de um anel graduado ([Liu02] pág. 53).

Um fato importante sobre $\mathbb{P}^n_k$ é com relação ao seu grupo de automorfismos:

Teorema 1.2.5 ([Har77] pág.151)**.** $\mathrm{Aut}_k(\mathbb{P}^n_k) = \mathrm{PGL}_n(k)$.

Outro objeto que usaremos no último capítulo serão as variedades abelianas. A "grosso modo" uma variedade abeliana (sobre $\mathbb{C}$) é um toro com certas propriedades.

Definição 1.2.6. *Um toro complexo n-dimensional sobre $\mathbb{C}$ é o quociente de uma espaço vetorial complexo V de dimensão n por um reticulado de posto n.*

Definição 1.2.7 ([CS86]; pág.85)**.** *Uma variedade abeliana X sobre $\mathbb{C}$ é um toro complexo que admite um forma Hermitiana ω não-degenerada tal que $Im(\omega)$ é inteira sobre o reticulado.*

Quando o corpo k é qualquer temos:

Definição 1.2.8 ([CS86] pág.104)**.** *Uma variedade abeliana X sobre k é uma variedade própria sobre k com uma aplicação multiplicação $m : X \times X \to X$ e uma aplicação inversão ambos morfismos de variedades.*

Exemplo 1.2.9.

1. Em dimensão 1, as variedades abelianas são exatamente as curvas elípticas.

2. Uma variedade jacobiana é um toro complexo de dimensão g associada a uma curva de gênero g. Mostra-se então que variedades jacobianas são variedades abelianas (para o caso de variedades jacobianas sobre $\mathbb{C}$, ver [BL04] pág.315).

As variedades abelianas são "especiais" por causa de sua estrutura.

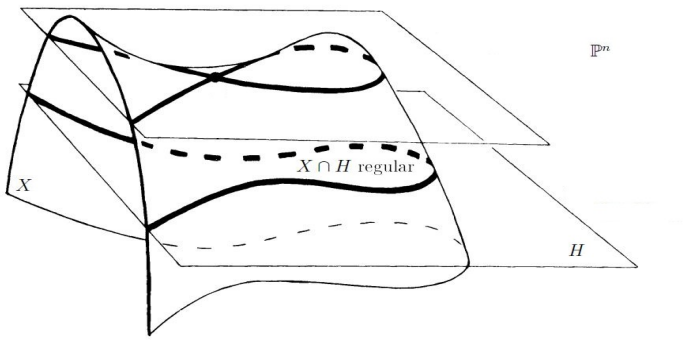
Teorema 1.2.10 ([CS86] pág.113)**.** *Uma variedade abeliana X sobre k é uma variedade projetiva sobre k, ou seja, existe um mergulho $X \to \mathbb{P}^n_k$ para algum $n > 0$.*

Essa é uma das principais propriedades das variedades abelianas que usaremos. No caso $k = \mathbb{C}$, esse é o Teorema de Lefschetz, que pode ser encontrado em [Deb05] pág.57 ou [Mum08] pág.28. Para um corpo qualquer, podemos citar [Mila] pág.27 e [Har77] pág.158.

Sabemos que todo automorfismo de uma variedade abeliana é o produto de uma translação (por um ponto da variedade) por um automorfismo da variedade preservando a estrutura de grupo (ver [Lan83] Teorema 4 pág.24). Quando a variedade abeliana é polarizada (a grosso modo é uma isogenia entre a variedade abeliana e seu dual; no caso complexo, uma variedade abeliana polarizada é um toro complexo com uma forma Hermitiana ω não-degenerada tal que $\mathrm{Im}(\omega)$ é inteira sobre o reticulado; para mais detalhes ver [Mila] pág.34 e 53), ela tem apenas um número finito de automorfismos que preservam a estrutura de grupo ([Mila] Teorema 14.4 pág.62). Assim, no caso de variedades abelianas polarizadas, quase todo automorfismo da variedade é uma translação por ponto. Esses serão os automorfismos usados no Capítulo Quatro.

Um argumento que usaremos no último capítulo é com relação a interseção $X \cap H$, de um hiperplano H com um esquema projetivo X, ser não singular e irredutível, ou seja, quando $X \cap H$ é um divisor primo (para um estudo sobre divisores ver [Har77] pág.129 e [Liu02] pág.252). Para isso ser uma "boa" propriedade, gostaríamos que quase todo hiperplano de $\mathbb{P}^n_k$ satisfizesse essa propriedade em algum sentido: isso será o *Teorema de Bertini*. Além disso, veremos o *teorema de Kronecker*, que permite tomar pontos com órbitas densas no toro. Ambos teoremas serão usados somente no último capítulo.

Teorema 1.2.11 (Teorema de Bertini; [Har77] pág.179)**.** *Seja X uma subvariedade regular (não singular) fechada de $\mathbb{P}^n_k$, onde k é um corpo algebricamente fechado. Então, existe um hiperplano $H \subset \mathbb{P}^n_k$, não contido em X e tal que o esquema $H \cap X$ é regular em todo ponto. Além disso, o conjunto dos hiperplanos com essa propriedade é um subconjunto denso do sistema linear completo $|H|$, considerado como um espaço projetivo. Além disso, se* $\dim X \geq 2$ *então $H \cap X$ é irredutível.*



Quando a dimensão de X é 1 é fácil ver que em geral $X \cap H$ não será irredutível. Por exemplo, se X é uma curva elíptica, em geral uma reta interceptará a curva em mais de um ponto (*Teorema de Bézout*) e portanto não será irredutível.

No caso que trataremos no Capítulo Quatro, o divisor irredutível $X \cap H$ será um polo. Por um polo entenderemos:

Definição 1.2.12 (Polo)**.** *Sejam X um esquema noetheriano integral separado regular sobre k, D um subesquema fechado integral de codimensão* 1 *(ou seja, um divisor) e F o corpo de funções de X. Seja $g \in F$. Diremos que g tem um polo ao longo de D (ou simplesmente D é um polo de g) se $v_D(g) < 0$, onde v_D é a valorização associada a D.*

Por último, o teorema de Kronecker, que assim como o Teorema de Bertini, dá uma certa condição de densidade.

Teorema 1.2.13 ([MMST11] pág.351). *Seja* $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$. *Suponha que* $1, \alpha_1, \ldots, \alpha_n$ *sejam linearmente independentes sobre* $\mathbb{Q}$. *Então,*

$$Y = \{k\alpha + e_1 m_1 + \cdots + e_n m_n \mid k \in \mathbb{N},\ m_1, \ldots, m_n \in \mathbb{Z}\}$$

é denso em $\mathbb{R}^n$, *onde os* e_i*'s são da base canônica do* $\mathbb{R}^n$.

1.3 Geometricamente irredutível, reduzido e integral

Ao trabalharmos com esquemas, mais precisamente com variedades algébricas, queremos que algumas de suas propriedades, como por exemplo irredutibilidade e redutibilidade, se mantenham após uma *mudança de base* (definição ver [Liu02] pág.78). Essas propriedades estão diretamente ligadas ao caso algébrico, onde podemos ter uma álgebra reduzida e queremos que após uma mudança de base ela continue reduzida. São essas características que serão apresentadas nesta seção, tanto no caso de variedades como no caso de álgebras. Inicialmente, vamos encontrar condições sobre uma extensão L/k ou sobre o corpo k, para que $L \otimes_k L'$ seja domínio, onde L'/k é uma extensão de corpos qualquer. Depois, faremos a ligação dessa propriedade com a de uma álgebra ou variedade ser geometricamente integral. A propriedade "geometricamente integral" é essencial neste trabalho e por isso, será detalhadamente discutida. As principais referências são [Car, Sta, Lan02]. Começamos com algumas definições.

Definição 1.3.1. *Seja* L/k *uma extensão de corpos.*

1. L *é separável sobre* k, *ou a extensão* L/k *é separável, se para toda subextensão* $k \subset L' \subset L$, *com* L' *finitamente gerada sobre* k, *existe uma base de transcendência* $\{x_i\}_{i \in I}$ *de* L'/k *tal que a extensão* $L'/k(x_i; i \in I)$ *é uma extensão algébrica separável.*

2. k *é separavelmente algebricamente fechado se todo elemento em* $\overline{k}$ *separável sobre* k *pertence a* k. *Quando* k *é perfeito,* k *é separavelmente algebricamente fechado se, e somente se,* k *é algebricamente fechado. Quando* $\mathrm{char}(k) > 0$ *então* k *é separavelmente algebricamente fechado se, e somente se,* $\overline{k}/k$ *é uma extensão puramente inseparável. Exemplificando, se* F *é um corpo qualquer, considere seu fecho separável* F^s *em* $\overline{F}$. *Qualquer subextensão* $F^s \subset K \subset \overline{F}$ *é separavelmente algebricamente fechada.*

3. L/k *é primária se o fecho algébrico de* k *em* L *é uma extensão puramente inseparável de* k. *Isso significa que para todo* $a \in L$ *algébrico sobre* k, *existe um* $n \geq 0$ *tal que* $a^{p^n} \in k$.

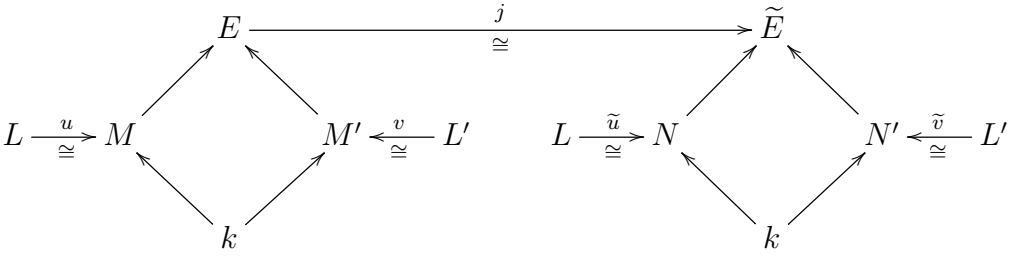
4. *L/k é regular se ela é separável e primária. Em particular, k é algebricamente fechado em L.*

Definição 1.3.2. *Seja k um corpo.*

1. *Seja Ω/k uma extensão de corpos e sejam A, B duas k-subálgebras de Ω. A e B são linearmente disjuntos sobre k em Ω se o mapa $A \otimes_k B \to \Omega$ dado por $\sum_i a_i \otimes b_i \mapsto \sum_i a_i b_i$ é injetivo (em particular, $A \otimes_k B$ é um domínio).*

2. *Seja Ω/k uma extensão de corpos e sejam $L, L'/k$ duas subextensões de Ω. L e L' são algebricamente disjuntas sobre k em Ω se todo subconjunto B de L que é algebricamente independente sobre k ainda é algebricamente independente sobre L'. Essa propriedade é simétrica em L e L'.*

3. *Sejam $L, L'/k$ duas extensões de corpos. Uma extensão composta de L e L' sobre k, denotada por $C = (E, u, v)$, é formada por uma extensão de corpos E/k gerada por duas subextensões M e M' algebricamente disjuntas sobre k e por dois k-isomorfismos $u : L \to M$ e $v : L' \to M'$. Duas extensões compostas $C = (E, u, v)$ e $\widetilde{C} = (\widetilde{E}, \widetilde{u}, \widetilde{v})$ (a segunda gerada por N e N') são equivalentes (ou de mesmo tipo) se existe um k-isomorfismo $j : E \to \widetilde{E}$ tal que $\widetilde{u} = j \circ u$ e $\widetilde{v} = j \circ v$, ou seja, se existe um k-isomorfismo $j : E \to \widetilde{E}$ (necessariamente único) estendendo os isomorfismos $f = \widetilde{u} \circ u^{-1} : M \to N$ e $g = \widetilde{v} \circ v^{-1} : M' \to N'$.*



Sobre essas definições, temos as seguintes observações:

Observação 1.3.3.

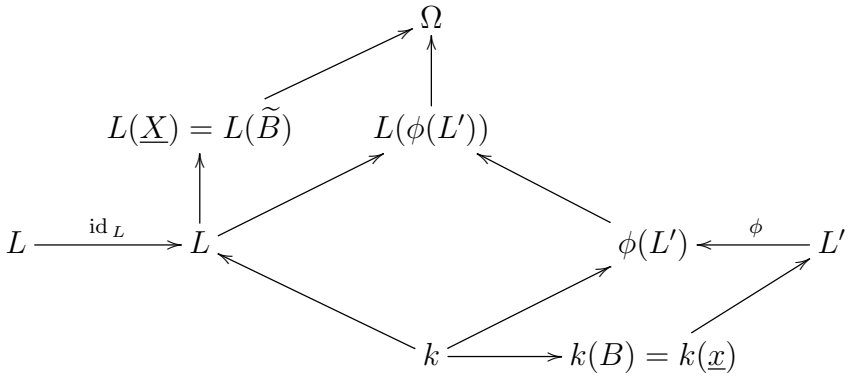
1. Sempre que nos referirmos a linearmente disjunto, algebricamente disjunto ou ainda ao fecho algébrico de um corpo dentro de outro, consideraremos que todos os corpos (ou álgebras) envolvidos são subextensões de uma mesma extensão do corpo base.

2. Note que se k é algebricamente fechado em L então L/k é primária. Quando k é perfeito ou L/k é separável, se L/k é primária então k é algebricamente fechado em L.

3. k é algebricamente fechado em L se, e somente se, $L \cap \overline{k} = k$, quando $L, \overline{k} \subset \Omega$ (ambos os sentidos são direto da definição de algebricamente fechado).

4. se A, B são linearmente disjuntos sobre k então $A \cap B = k$.

Observação 1.3.4. Sejam L e L' duas extensões de corpos de um corpo k. Podemos construir uma extensão composta de L e L' sobre k, de tal forma que imagens isomorfas de ambos estejam contidas em um mesmo corpo e que dentro desse "novo ambiente" elas sejam algebricamente disjuntas sobre k. Para isso, sejam B uma base de transcendência de L' sobre k e $\Omega = \overline{L(X_i; i \in I)}$, onde as indeterminadas X_i correspondem biunivocamente aos elementos $x_i \in B$. Escrevemos $\widetilde{B} = \{\underline{X}\} \subset \Omega$, onde a notação $\underline{X}$ indica uma t-upla. Identificamos $k(B) \subset L'$ (abuso de notação, onde $k(B)$ significa $k(\underline{x})$ para $B = \{\underline{x}\}$) a um subcorpo de Ω pela correspondência $x_i \leftrightarrows X_i$. Se id_L é a aplicação identidade de L em Ω e ϕ é uma $k(B)$-imersão de L' em Ω, então $C(\phi) \stackrel{def}{=} (L(\phi(L')), \mathrm{id}_L, \phi)$ é uma extensão composta de L e L', onde B é uma base de transcendência de $\phi(L')$ sobre k que é algebricamente independente sobre L. Por construção, L e $\phi(L')$ são algebricamente disjuntos sobre k.



A definição de linearmente disjunto tem as seguintes equivalências:

Lema 1.3.5. *Seja Ω/k uma extensão de corpos e sejam A, B duas k-subálgebras de Ω. São equivalentes:*

1. *A e B são linearmente disjuntos sobre k em Ω;*

2. *dadas bases $\{u_i\}$ e $\{v_j\}$ de A e B sobre k, respectivamente, temos que $u_i v_j$ são l.i. sobre k;*

3. *todo subconjunto finito de A que é linearmente independente sobre k é ainda linearmente independente sobre B (que é simétrico em A e B).*

Demonstração: Se $\{u_i\}$ e $\{v_j\}$ são bases de A e B sobre k, respectivamente, os elementos $u_i \otimes v_j$ formam uma base de $A \otimes_k B$ sobre k, direto das propriedades do produto tensorial.

(1) $\Rightarrow$ (2): como $A \otimes_k B \to \Omega$ é injetora, se $\sum_{i,j} a_{ij} u_i v_j = 0$, então $\sum_{i,j} a_{ij} u_i \otimes v_j = 0$ e portanto $a_{ij} = 0$ para todo i, j, pois $\{u_i \otimes v_j\}$ é uma base de $A \otimes_k B$.

(2) $\Rightarrow$ (3): suponha que $\{f_i\} \subset A$, para $1 \leq i \leq n$, é l.i. sobre k e considere $\sum_i b_i f_i = 0$ onde $b_i \in B$. Vamos mostrar que $b_i = 0$ para todo i. Considere as bases dadas no item (2). Além disso, escrevemos $\underline{b}, \underline{f}$ os vetores colunas formados pelos b_i's e f_i's respectivamente. Também escreva $\underline{b} = C\underline{v}$ e $\underline{f} = D\underline{u}$, onde C, D são as matrizes $n \times m$ (não necessariamente quadradas) de $\underline{b}$ e $\underline{f}$ nas bases de B e A respectivamente. Então,

$$\begin{aligned}
\langle \underline{b}, \underline{f} \rangle &= \langle C\underline{v}, D\underline{u} \rangle \\
&= \langle \underline{v}, C^t D\underline{u} \rangle \\
&= \langle \underline{v}, C^t D\underline{u} \rangle \\
&= \langle \sum v_i e_i, C^t D \sum u_j e_j \rangle \\
&= \sum v_i u_j \langle e_i, C^t D e_j \rangle,
\end{aligned}$$

onde os e_i's são da base canônica. Portanto, $\langle e_i, C^t D e_j \rangle = 0$ para todo i, j por hipótese, ou seja, $C^t D = 0$. Temos que $n = min\{m, n\}$. Como D é a matriz de um conjunto l.i. sobre k na base de A, temos que algum dos menores $E_{n\times n}$ de D é inversível. No produto $C^t D = 0$ (transpondo se necessário) cada vetor linha w_i de C^t forma um sistema $n \times n$ com E, a dizer, $Ew_i^t = 0$, ou seja, temos que w_i é o vetor nulo para todo i e consequentemente $C = 0$.

(3) $\Rightarrow$ (1): basta supor que em um elemento $\sum a_i \otimes b_i$ tomamos, por exemplo, os b_i's l.i. sobre k, ou seja, tomamos uma expressão minimal. A injetividade sai do fato que os b_i's ainda são l.i. sobre A. Isso encerra a prova.

■

1.3.1 Resultados gerais sobre corpos

Aqui, apresentaremos vários lemas que serão usados nas próximas subseções. Em sua maioria, são resultados gerais sobre extensões de corpos. O objetivo dessa seção é mostrar as possíveis relações entre o 'tipo de extensão' que consideramos e a propriedade 'linearmente disjunto'. O principal resultado é o Teorema 1.3.8.

O primeiro lema mostra um caso em que duas extensões de um mesmo corpo k são linearmente disjuntas.

Lema 1.3.6. *Sejam k um corpo com $\mathrm{char}(k) = p > 0$, L/k uma extensão separável e M/k uma extensão puramente inseparável. Então, L e M são linearmente disjuntos sobre k.*

Demonstração: Note que podemos supor que L é finitamente gerado sobre k, pois a verificação de linearmente disjunto é sobre um subconjunto finito. Além disso, se $k \subset L' \subset L$ e $k \subset M \subset M(L')$, onde $M, L \subset \Omega$, então se L', M são linearmente disjuntos sobre k e $L, M(L')$ são linearmente disjuntos sobre L' então M, L são linearmente disjuntos sobre k. De fato, se $\{m_i\} \subset M$ é l.i. sobre k então $\{m_i\}$ é l.i. sobre L'. Mas, $M \subset M(L')$, ou seja, $\{m_i\}$ é l.i. sobre L, como queríamos. Note também que $M(L')/L'$ é puramente inseparável.

Como L/k é separável e L é finitamente gerado sobre k, encontramos uma subextensão $k \subset k(\underline{x}) \subset L$ tal que $k(\underline{x})/k$ é puramente transcendente e $L/k(\underline{x})$ é algébrico separável. Portanto, pela observação anterior, precisamos provar o lema nos seguintes dois casos: quando temos uma extensão finita separável $k(\theta)/k$ e M/k puramente inseparável (lembramos que L é o limite direto de extensões L_i com $[L_i : k(\underline{x})] < +\infty$); o segundo, é quando temos $k(x)/k$ uma extensão puramente transcendente e M/k puramente inseparável.

Seja $k(\theta)/k$ com θ algébrico separável sobre k e M/k puramente inseparável. Temos $k \subset k(\theta) \subset k^s$. Note que

$$k(\theta) \otimes_k M \cong (k[T]/(p(T))) \otimes_k M \cong M[T]/(p(T)),$$

onde $p(T)$ é o polinômio minimal de θ sobre k. Se $p = p_1 p_2$ sobre M, então p_1, p_2 tem coeficientes em M. Porém, p também se decompõe dessa forma sobre k^s, onde os coeficientes são polinômios nas raízes de p. Com isso, esses coeficientes estão em $k^s \cap M$. Mas, $k \subset k^s \cap M \subset k^s \cap k^{p^{-\infty}} = k$,[1] o que é absurdo pois p é irredutível sobre k. Portanto, $M[T]/(p(T))$ é corpo. Falta mostrar que o morfismo natural de $k(\theta) \otimes_k M$ em Ω é injetor; mas isso ocorre desde que $k(\theta) \otimes_k M$ é corpo e M injeta em Ω.

O outro caso é quando temos $k(\underline{x})/k$ puramente transcendente e M/k puramente inseparável. Primeiramente, note que $k[\underline{x}]$ e M são linearmente disjuntos sobre k. De fato, os elementos $\underline{x}^{\underline{\alpha}}$ formam uma base de $k[\underline{x}]$. Então, se $\sum m_i \underline{x}^{\underline{\alpha}} = 0$, com $m_i \in M$, então $\sum m_i^{p^n} (\underline{x}^{p^n})^{\underline{\alpha}} = 0$, com $m_i^{p^n} \in k$ para $n \gg 0$. Mas os $(\underline{x}^{p^n})^{\underline{\alpha}}$ continuam l.i. sobre k, o que mostra que $m_i^{p^n} = 0$ para todo i, ou seja, $m_i = 0$. Agora, se consideramos $\{m_i\}$ l.i. sobre k e uma expressão da forma $\sum f_i(\underline{x}) m_i = 0$, onde $f_i(\underline{x}) \in k(\underline{x})$, existe $g(\underline{x}) \in k[\underline{x}]$ tal que $\sum g(\underline{x}) f_i(\underline{x}) m_i = 0$ tem coeficientes em $k[\underline{x}]$. Portanto, $g(\underline{x}) f_i(\underline{x}) = 0$ para todo i, o que significa que $f_i(\underline{x}) = 0$ para todo i, como queríamos.

■

A proposição seguinte faz uma conexão entre "linearmente disjunto" e "separável". Mais adiante, veremos que esse resultado nos diz um pouco mais sobre a extensão L/k.

[1] a igualdade $K^s \cap K^{p^{-\infty}} = K$ é provada assim: se $a \in K^s \cap K^{p^\infty}$ então $a^{p^n} = b \in K$. Logo, o polinômio $P(T) = T^{p^n} - b$ tem a como única raiz, ou seja, $P_a(T) \mid P(T)$. Se $a \notin K$ então $P_a(T)$ tem pelo menos duas raízes distintas em $\overline{K}$, o que é um absurdo, portanto $a \in K$.

Proposição 1.3.7. *Seja L/k uma extensão de corpos e suponha* $\mathrm{char}(k) = p > 0$. *As seguintes condições são equivalentes:*

(i) L é linearmente disjunto de $k^{p^{-\infty}}$.

(ii) L é linearmente disjunto de $k^{p^{-m}}$, para algum $m \geq 1$.

(iii) L/k é separável.

Demonstração: De maneira direta $(i) \Rightarrow (ii)$. Pelo Lema 1.3.6 temos que $(iii) \Rightarrow (i)$. Para provar que $(ii) \Rightarrow (iii)$, podemos supor que L é finitamente gerado sobre k ou seja

$$L = k(\underline{x}) = k(x_1, \ldots, x_n).$$

Seja $r = \mathrm{trdeg}_k L$. Se $r = n$, acabou. Caso contrário, suponha sem perda de generalidade que $\{x_1, \ldots, x_r\}$ é uma base de transcendência e x_{r+1} é algébrico sobre $k(x_1, \ldots, x_r)$. Seja $f(X_1, \ldots, X_{r+1})$ um polinômio de menor grau tal que $f(x_1, \ldots, x_{r+1})$ é nulo. Afirmamos que nem todos x_i's, com $(i = 1, \ldots, r+1)$, aparecem em todo monômio de f como p-ésimas potências. Se todos eles aparecem, podemos escrever

$$f(\underline{X}) = \sum c_\alpha M_\alpha(\underline{X})^p,$$

onde $M_\alpha(\underline{X})$ são monômios em $X_1, \ldots, X_{r+1}$ e $c_\alpha \in k$. Isso implicaria que os monômios $M_\alpha(\underline{x})$ são linearmente dependentes sobre $k^{1/p}$ (tomando a p-ésima raiz da equação $\sum c_\alpha M_\alpha(\underline{x})^p = 0$). Contudo, os $M_\alpha(\underline{x})$ são linearmente independentes sobre k (pois caso contrário poderíamos pegar uma equação em $x_1, \ldots, x_{r+1}$ de grau menor) e então nós obtemos uma contradição, pois $k(\underline{x})$ e $k^{1/p}$ são linearmente disjuntos. Suponha, renomeando se necessário, que X_1 aparece em $f(\underline{X})$ mas não é p-ésima potência em todo monômio. Sabemos que $f(\underline{X})$ é irredutível em $k[X_1, \ldots, X_{r+1}]$ e portanto $f(\underline{x}) = 0$ é uma equação irredutível para x_1 sobre $k(x_2, \ldots, x_{r+1})$. Como X_1 não aparece sempre como uma p-ésima potência, essa equação é separável para x_1 sobre $k(x_2, \ldots, x_{r+1})$, ou seja, x_1 é algébrico separável sobre $k(x_2, \ldots, x_{r+1})$. Consequentemente, x_1 é algébrico separável sobre $k(x_2, \ldots, x_n)$. Se $x_2, \ldots, x_n$ é uma base de transcendência, acabou. Caso contrário, temos que x_2 é separável sobre $k(x_3, \ldots, x_n)$. Então, $k(\underline{x})$ é separável sobre $k(x_3, \ldots, x_n)$. Indutivamente, esse processo termina quando obtermos uma base de transcendência. Isso encerra a prova.

■

O próximo resultado nos dará uma importante caracterização de uma extensão regular.

Teorema 1.3.8. *Seja L/k uma extensão de corpos. Então, L e $\overline{k}$ são linearmente disjuntos sobre k se, e somente se, L/k é regular.*

Demonstração: Suponha que L e $\overline{k}$ são linearmente disjuntos sobre k. Pela Proposição 1.3.7 temos que L/k é separável. Como L e $\overline{k}$ são linearmente disjuntos sobre k, então $L \cap \overline{k} = k$ (Observação 1.3.3) e assim k é algebricamente fechado em L. Portanto, L/k é regular.

Suponha que L/k é regular e vamos mostrar que L e $\overline{k}$ são linearmente disjuntos sobre k. Podemos supor que L é finitamente gerado sobre k e é suficiente mostrar que L é linearmente disjunto de uma extensão k'/k algébrica finita (mesmo argumento usado na demonstração do Lema 1.3.6).

Agora, se k'/k também é separável, então escreva $k' = k(\theta)$, onde θ é algébrico sobre k, ou seja, $k' = k[T]/(p(T))$, onde $p(T)$ é um polinômio minimal de θ sobre k. Então, L e k' são linearmente disjuntos sobre k. De fato, temos que $L \otimes_k k' \cong L[T]/(p(T))$ e $p(T)$ é ainda irredutível sobre L. Caso contrário, temos $p = p_1 p_2$, onde os coeficientes de p_1 e p_2 pertencem a L. Como essa decomposição também vale em $\overline{k}$, os coeficientes também pertencem a $\overline{k}$ e portanto a k (pois k é algebricamente fechado em L). Absurdo.

Suponha que k'/k não é separável. Seja $E = k_{\text{sep}} \subset k'$ o fecho separável de k em k'. Para mostrar que L e k' são linearmente disjuntos sobre k, é suficiente mostrar que $L(E)$ e k' são linearmente disjuntos sobre E e L e E são linearmente disjuntos sobre k, pelo mesmo argumento usado na demonstração do Lema 1.3.6. Como L/k e E/k são separáveis, pelo caso anterior L e E são linearmente disjuntos sobre k. Note que $L(E)/E$ é separável: se $\{\underline{x}\}$ é uma base de transcendência de L/k então ela também é de $L(E)/E$, pois L e E são linearmente disjuntos sobre k. Assim, $E(\underline{x})/E$ é separável. Além disso, todo elemento de L é separável sobre $k(\underline{x})$ e portanto sobre $E(\underline{x})$. Isso mostra que $L(E)/E(\underline{x})$ é separável. Pelo Lema 1.3.6 temos que $L(E)$ e k' são linearmente disjuntos sobre E. Isso encerra a prova

■

Podemos obter informações importantes sobre a extensão L/k quando k é perfeito:

Lema 1.3.9. *Se k é perfeito então toda extensão de k é separável.*

Demonstração: Como todo elemento é uma p-ésima potência, então $k = k^{1/p}$. Se L/k é uma extensão qualquer, então L e $k^{1/p}$ são linearmente disjuntos sobre k. A Proposição 1.3.7 nos diz que L/k é separável (de modo trivial quando $\text{char}(k) = 0$).

■

O resultado a seguir será usado apenas no Lema 1.3.11.

Lema 1.3.10. *Sejam L/k uma extensão algébrica separável, $\alpha \in L$ e $P(T)$ um polinômio separável sobre k tal que $P(\alpha) = 0$. Suponha que $\text{char}(k) = p > 0$. Se os coeficientes de $P(T)$ são p-ésimas potências em k então α é uma p-ésima potência em L.*

Demonstração: Escreva $P(T) = T^d + a_1T^{d-1} + \ldots + a_d$ o polinômio separável de α sobre k e suponha que $a_i = b_i^p$. Então, o polinômio $Q(T) = T^d + b_1T^{d-1} + \ldots + b_d$ é um polinômio mônico, com coeficientes em k e anulado por $\alpha^{1/p}$. Como a extensão $L(\alpha^{1/p})/L$ é puramente inseparável, basta mostramos que $Q(T)$ é separável e obteremos que $L(\alpha^{1/p}) = L$, como queríamos. Para isso, note que se γ é raiz de $P(T)$, então, $\gamma^{1/p}$ é raiz de $Q(T)$ e portanto $Q(T)$ é separável.

■

O próximo lema será usado apenas na demonstração do Teorema 1.3.18.

Lema 1.3.11. *Seja k um corpo. Seja L/k uma extensão finitamente gerada. Então, existe um diagrama*

$$\begin{array}{ccc} L & \longrightarrow & L' \\ \uparrow & & \uparrow \\ k & \longrightarrow & k' \end{array}$$

onde k'/k e L'/L são extensões finitas puramente inseparáveis tais que L'/k' é uma extensão separável.

Demonstração: Escolha $x_1, \ldots, x_r$ uma base de transcendência de L/k. Como L/k é finitamente gerada, então a extensão $L/k(x_1, \ldots, x_r)$ é finita. Seja $k(x_1, \ldots, x_r) \subset L_{\text{sep}} \subset L$ o fecho separável de $k(\underline{x})$ em L, ou seja, temos que $L_{\text{sep}}/k(x_1, \ldots, x_r)$ é separável e L/L_{sep} é puramente inseparável. Se $L = L_{\text{sep}}$ então acabou (por exemplo quando $\text{char}(k) = 0$). Suponha que $\text{char}(k) = p > 0$ e seja $d = [L : L_{\text{sep}}]$. Vamos provar por indução em d.

Suponha que $d > 1$. Escolha um $\beta \in L$ tal que $\alpha = \beta^p \in L_{\text{sep}}$ e $\beta \notin L_{\text{sep}}$. Seja $P = T^d + a_1T^{n-1} + \ldots + a_d$ o polinômio minimal de α sobre $k(x_1, \ldots, x_r)$. Seja k'/k uma extensão finita puramente inseparável obtida incluindo as p-ésimas potências de todos os coeficientes que aparecem em todos os a_i's, tal que cada a_i é uma p-ésima potência em $k'(x_1^{1/p}, \ldots, x_r^{1/p})$. Seja L' o corpo levantado no diagrama

$$\begin{array}{ccc} L & \longrightarrow & L' \\ \uparrow & & \uparrow \\ k(x_1, \ldots, x_r) & \longrightarrow & k'(x_1^{1/p}, \ldots, x_r^{1/p}) \end{array}$$

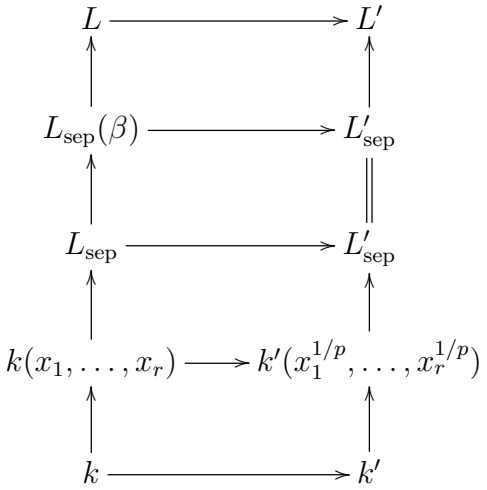
onde $L' = L(k'(x_1^{1/p}, \ldots, x_r^{1/p}))$ é o menor corpo gerado por L e $k'(x_1^{1/p}, \ldots, x_r^{1/p})$ sobre $k(x_1, \ldots, x_r)$ dentro de $\overline{L}$. Seja

$$k'(x_1^{1/p}, \ldots, x_r^{1/p}) \subset L'_{\text{sep}} \subset L',$$

o fecho separável de $k'(x_1^{1/p}, \ldots, x_r^{1/p})$ em L'.

Afirmamos que $L'_{\text{sep}} = L_{\text{sep}}(k'(x_1^{1/p}, \ldots, x_r^{1/p}))$. De fato, se $a \in L'$, então $a^p \in L$ e portanto, $a^{p^n} \in L_{\text{sep}}$, ou seja, $a^{p^n} \in L_{\text{sep}}(k'(x_1^{1/p}, \ldots, x_r^{1/p}))$ mostrando que a extensão $L'/L_{\text{sep}}(k'(x_1^{1/p}, \ldots, x_r^{1/p}))$ é puramente inseparável. Como L'/L'_{sep} é puramente inseparável, basta mostrar que $L_{\text{sep}}(k'(x_1^{1/p}, \ldots, x_r^{1/p})) \subset L'_{\text{sep}}$ e isso encerra. Como $k'(x_1^{1/p}, \ldots, x_r^{1/p}) \subset L'_{\text{sep}}$, resta mostrar que $L_{\text{sep}} \subset L'_{\text{sep}}$. Para isso, seja $a \in L_{\text{sep}}$ e sejam P_a o polinômio minimal de a sobre $k(x_1, \ldots, x_r)$ e P'_a o polinômio minimal de a sobre $k'(x_1^{1/p}, \ldots, x_r^{1/p})$. Sobre $k'(x_1^{1/p}, \ldots, x_r^{1/p})$, temos que $P'_a \mid P_a$, ou seja, P'_a é separável sobre $k'(x_1^{1/p}, \ldots, x_r^{1/p})$ e portanto $a \in L'_{\text{sep}}$.

O elemento $\alpha \in L_{\text{sep}} \subset L'_{\text{sep}}$ tem um polinômio separável P sobre $k'(x_1^{1/p}, \ldots, x_r^{1/p})$ tal que todos seus coeficientes são p-ésimas potências em $k'(x_1^{1/p}, \ldots, x_r^{1/p})$. Pelo Lema 1.3.10, temos que $\alpha = (\beta)^p$, com $\beta \in L'_{\text{sep}}$. Em outras palavras, nós obtemos uma torre de corpos



Com isso, chegamos na situação em que $[L' : L'_{\text{sep}}] < [L : L_{\text{sep}}]$. Por indução, podemos encontrar k''/k' e L''/L', com as propriedades do enunciado, para a extensão L'/k'. Então, as extensões k''/k e L''/L funcionam para a extensão L/k. Isso prova o lema.

■

1.3.2 Álgebras geometricamente reduzidas

Nesta subseção, encontraremos condições para que uma álgebra seja geometricamente reduzida e mostraremos como podemos verificar essa propriedade. O principal resultado é o Teorema 1.3.18.

Definição 1.3.12. *Sejam k um corpo e S uma k-álgebra. S é geometricamente reduzida sobre k se a L-álgebra $S \otimes_k L$ é reduzida para toda extensão de corpos L/k.*

É claro que nem toda álgebra reduzida é geometricamente reduzida. Veja o exemplo 1.3.35 (que também serve para o caso de álgebras).

Os próximos dois lemas funcionarão como "redutores de casos" para algumas demonstrações.

Lema 1.3.13. *Sejam k um corpo e R, S k-álgebras. Se $R \otimes_k S$ não é reduzida (ou, contém um divisor de zero não-nulo), então existem subálgebras finitamente geradas $R' \subset R$ e $S' \subset S$ tais que $R' \otimes_k S'$ não é reduzida (ou, contém um divisor de zero não-nulo).*

Demonstração: Suponha que $z \in R \otimes_k S$ é nilpotente. Podemos escrever $z = \sum x_i \otimes y_i$ como uma soma finita. Tome R' a k-subálgebra gerada pelos x_i's e S' a k-subálgebra gerada pelos y_i's. Quando $z = \sum x_i \otimes y_i$ é divisor de zero não nulo, existe $w = \sum a_i \otimes b_i \in R \otimes_k S$ não nulo tal que $zw = 0$. De modo análogo ao anterior, tome R' a k-subálgebra gerada pelos x_i's e a_i's e S' a k-subálgebra gerada pelos y_i's e b_i's.

■

Antes do próximo resultado, temos o seguinte lema técnico:

Lema 1.3.14. *Seja p um ideal primo minimal de um anel R. Então, todo elemento do ideal maximal de R_p é nilpotente. Além disso, se R é reduzido, então R_p é corpo.*

Demonstração: R_p é um anel local com ideal maximal $m = pR_p$. Como p é minimal, então o único primo de R_p é m, ou seja, $\sqrt{0} = m$. Agora, se R é reduzido, então $m = pR_p = (0)$ e portanto R_p é corpo.

■

O próximo lema nos mostra que os ideais primos são importantes quando falamos sobre álgebras reduzidas. Além disso, quando queremos mostrar que uma álgebra reduzida A é geometricamente reduzida, esse lema nos mostrará que em certos casos podemos assumir que A é um corpo.

Lema 1.3.15. *Sejam k um corpo e S uma k-álgebra reduzida. Suponha que S_p (um corpo pelo Lema 1.3.14) é geometricamente reduzido para todo ideal primo minimal p de S. Então, S é geometricamente reduzida. Com isso, podemos assumir que S é um corpo.*

Demonstração: Como S é reduzida, então o mapa natural

$$S \to \prod_{p \,\text{minimal}} S_p$$

é injetivo. Se L/k é uma extensão de corpos, então os mapas

$$S \otimes_k L \to (\prod_{p \,\text{minimal}} S_p) \otimes_k L \to \prod_{p \,\text{minimal}} (S_p \otimes_k L)$$

são todos injetivos. O primeiro é porque L é plano sobre k. Já o segundo, é injetivo pois L é um k-módulo livre. De fato, escreva $L = \bigoplus_i ke_i$. Temos que

$$(\prod_p S_p) \otimes_k (\bigoplus_i ke_i) \cong \bigoplus_i \prod_p (S_p \otimes_k ke_i) \cong \prod_p \bigoplus_i (S_p \otimes_k ke_i),$$

onde o segundo isormofismo é dado pela transposição de matrizes[2]. Como S_p é geometricamente reduzido para todo primo minimal, o produto também é reduzido. Portanto, $S \otimes_k L$ é reduzido como subanel de um anel reduzido e isso mostra também a segunda afirmação.

■

Quando temos uma extensão separável, obtemos algumas consequências importantes, como mostra o seguinte

Lema 1.3.16. *Sejam k um corpo e S uma k-álgebra reduzida. Seja L/k uma extensão separável. Então, $S \otimes_k L$ é reduzida.*

Demonstração: Pelo Lema 1.3.13 podemos supor que L e S são finitamente gerados sobre k. Como L/k é separável e finitamente gerada, seja $\{\underline{x}\}$ uma base de transcendência finita sobre k e θ um elemento de L algébrico e separável sobre $k(\underline{x})$ tal que $L = k(\underline{x})(\theta)$. Seja $p(T)$ o polinômio minimal separável de θ sobre $k(\underline{x})$. Além disso, podemos supor que S é um corpo pelo Lema 1.3.15. Então,

$$S \otimes_k L \cong S \otimes_k k(\underline{x})(\theta) \cong S \otimes_k \frac{k(\underline{x})[T]}{(p(T))} \cong \frac{(S \otimes_k k(\underline{x}))[T]}{(p(T))},$$

onde $S \otimes_k k(\underline{x})$ é domínio, pois é uma localização do domínio $S \otimes_k k[\underline{x}]$. Note que o mapa

$$\frac{(S \otimes_k k(\underline{x}))[T]}{(p(T))} \to \frac{\mathrm{Frac}(S \otimes_k k(\underline{x}))[T]}{(p(T))},$$

é injetor, pois, caso contrário, teríamos $f(T) \in (S \otimes_k k(\underline{x}))[T]$ e $g(T) \in \mathrm{Frac}(S \otimes_k k(\underline{x}))[T]$ tais que $f = pg$. Dividindo f por p, obtemos um polinômio com coeficientes em $S \otimes_k k(\underline{x})$ pois p é mônico. Portanto, $\overline{f} = 0$ em $(S \otimes_k k(\underline{x}))[T]/(p(T))$.

Como o polinômio $p(T)$ é separável, segue do Teorema Chinês dos Restos que $(\mathrm{Frac}(S \otimes_k k(\underline{x}))[T])/(p(T))$ é um produto de corpos, ou seja, reduzido. Isso encerra a prova.

■

O próximo lema nos mostrará a relação entre uma extensão de corpos L/k que é separável e a propriedade geometricamente reduzido. Além disso, ele complementa a Proposição 1.3.7.

[2]olhamos os elementos de $\prod_p \bigoplus_i (S_p \otimes_k ke_i)$ como matrizes com infinitas linhas não nulas, mas em cada linha apenas um número finito de colunas são não nulas, e analogamente para o termo $\bigoplus_i \prod_p (S_p \otimes_k ke_i)$; mesmo não sendo um morfismo de anéis, essa operação é compatível com o produto.

Lema 1.3.17. *Seja k um corpo de característica $p > 0$. Seja L/k uma extensão de corpos. São equivalentes:*

1. *L/k é separável.*
2. *$L \otimes_k k^{1/p}$ é reduzido.*
3. *L é geometricamente reduzido.*

Demonstração: (1) $\Rightarrow$ (3): segue do Lema 1.3.16. (3) $\Rightarrow$ (2): por definição. (2) $\Rightarrow$ (1): podemos assumir que L é finitamente gerado. Precisamos encontrar uma base de transcendência separável de L/k.

Seja $\{\underline{x}\} = \{x_1, \cdots, x_r\}$ uma base de transcendência de L/k tal que o grau de inseparabilidade de $L/k(\underline{x})$ é minimal. Se $L/k(\underline{x})$ é separável, acabou. Caso contrário, existe $\alpha \in L$ que não é separável sobre $k(\underline{x})$. Seja $Q(T)$ o polinômio minimal de α sobre $k(\underline{x})$. Como α não é separável, Q é um polinômio em T^p. Limpando denominadores, obtemos um polinômio irredutível

$$G(\underline{X}, T) \in k[\underline{X}, T],$$

tal que $G(\underline{x}, \alpha) = 0$ em L. Isso significa que $k[\underline{X}, T]/(G) \subset L$.

Afirmamos que $\frac{dG}{dX_i}$ não é identicamente nulo para algum i. Caso contrário, G é um polinômio em $\underline{X}^p, T^p$, ou seja, $G^{1/p} \in k^{1/p}[\underline{X}, T]$ seria levado em um elemento nilpotente não nulo de $k^{1/p} \otimes_k L$. Assim, sem perda de generalidade, suponha que $\frac{dG}{dX_1} \neq 0$. Então, x_1 é algébrico separável sobre $k(\underline{x}, \alpha)$ e $x_2, \cdots, x_r, \alpha$ é uma base de transcendência de L/k. Portanto, o grau de inseparabilidade de $L/k(x_2, \cdots, x_r, \alpha)$ é menor que o de $L/k(\underline{x})$, contradição.

■

Vejamos agora o principal resultado dessa subseção, que nos mostrará que para verificar se uma k-álgebra é geometricamente reduzida não precisamos olhar para todas as extensões de k.

Teorema 1.3.18. *Sejam k um corpo e S uma k-álgebra. São equivalentes:*

1. *$S \otimes_k M$ é reduzido para qualquer extensão finita puramente inseparável M/k;*
2. *$S \otimes_k k^{1/p}$ é reduzido;*
3. *$S \otimes_k k^{p^{-\infty}}$ é reduzido;*
4. *$S \otimes_k \overline{k}$ é reduzido;*
5. *S é geometricamente reduzida sobre k.*

Demonstração: Primeiramente note que qualquer extensão puramente inseparável finita L'/k mergulha em $k^{p^{-\infty}}$. Além disso, temos que $k^{1/p} \hookrightarrow k^{p^{-\infty}} \hookrightarrow \overline{k}$. Portanto, como S é plano sobre k, obtemos $5 \Rightarrow 4 \Rightarrow 3 \Rightarrow 2$ e $3 \Rightarrow 1$. Para finalizar, vamos mostrar $1 \Rightarrow 5$ e $2 \Rightarrow 5$.

$1 \Rightarrow 5$. Suponha que vale 1. Seja L/k uma extensão de corpos e vamos mostrar que $S \otimes_k L$ é reduzido. Pelo Lema 1.3.13 podemos supor que L é finitamente gerado sobre k. Escolha um diagrama

$$\begin{array}{ccc} L & \longrightarrow & L' \\ \uparrow & & \uparrow \\ k & \longrightarrow & k' \end{array}$$

onde k'/k e L'/L são extensões finitas puramente inseparáveis tais que L'/k' é uma extensão separável, como no Lema 1.3.11. Por hipótese, $S \otimes_k k'$ é reduzido. Pelo Lema 1.3.16, $S \otimes_k L'$ é reduzido. Portanto, $S \otimes_k L$ é reduzido (mesmo argumento: S é plano sobre k e $S \otimes_k L'$ é reduzido).

$2 \Rightarrow 5$. Note que podemos supor que S é corpo pelo Lema 1.3.15. O resultado segue do Lema 1.3.17.

■

Finalizamos essa subseção com um lema.

Lema 1.3.19. *Seja k um corpo perfeito. Qualquer k-álgebra reduzida é geometricamente reduzida sobre k. Se R e S são duas k-álgebras reduzidas então $R \otimes_k S$ é reduzida.*

Demonstração: A primeira afirmação é uma consequência direta do Teorema 1.3.18. Vejamos a segunda afirmação. Temos que R, S são geometricamente reduzidos. Além disso, podemos supor que R é um corpo pelo Lema 1.3.15, o que encerra a prova.

■

1.3.3 Álgebras geometricamente irredutíveis e integrais

Nessa subseção, apresentaremos condições para que uma álgebra seja geometricamente irredutível. Os principais resultados são os Teoremas 1.3.25 e 1.3.31. Começamos com uma definição.

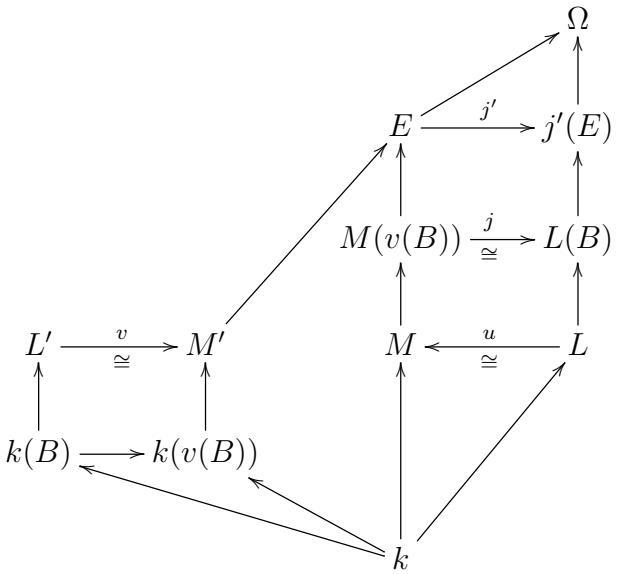
Definição 1.3.20. *Sejam k um corpo e S uma k-álgebra. S é geometricamente irredutível sobre k se* $\mathrm{Spec}(S \otimes_k L)$ *é irredutível para toda extensão de corpos L/k.*

É claro que nem toda álgebra irredutível é geometricamente irredutível. Veja os exemplos 1.3.34 e 1.3.35 (que também servem para o caso de álgebras).

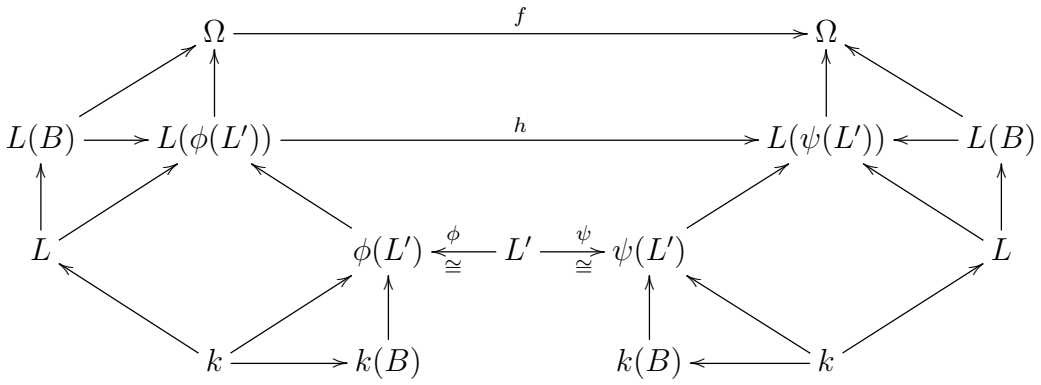
Vamos enunciar quatro resultados, todos encontrados em [Car], que serão usados na demonstração do Teorema 1.3.25.

Proposição 1.3.21. *Sejam L e L' duas extensões de k, B uma base de transcendência de L' sobre k e $\Omega = \overline{L(B)}$ (usaremos esse abuso de notação mais vezes, onde $L(B)$ significa $L(\underline{x})$ para $B = \{\underline{x}\} = \{x_1, x_2, \ldots\}$ e depois tomamos um fecho algébrico de $L(B)$). Toda extensão composta de L e L' é equivalente a uma extensão composta da forma $C(\phi) = (L(\phi(L')), \mathrm{id}_L, \phi)$, onde ϕ é uma $k(B)$-imersão de L' em Ω. $C(\phi)$ e $C(\phi')$ são equivalentes se, e somente se, existe um $L(B)$-automorfismo f de Ω tal que $\phi' = f \circ \phi$.*

Demonstração: Seja $C = (E, u, v)$ uma extensão composta de L e L'. Vamos mostrar primeiramente que C é equivalente a uma extensão $C(\phi)$. Como as extensões $M = u(L)$ e $M' = v(L')$ contidas em (e que geram) E são algebricamente disjuntas, então $v(B)$ é algebricamente independente sobre M (pois $v(B)$ é algebricamente independente sobre k), ou seja, $M(v(B))/M$ é puramente transcendente e E é algébrico sobre $M(v(B))$ (M e M' geram E, $M \subset M(v(B))$ e M' é algébrico sobre $k(v(B))$). Como B é algebricamente independente sobre L, existe um k-isomorfismo $j : M(v(B)) \to L(B)$ que coincide com u^{-1} sobre M e é tal que $j(v(x)) = x$ para todo $x \in B$ (ou seja, estendemos de modo natural u para $M(v(B))$ sobre $L(B)$). Como Ω é algebricamente fechado e E é algébrico sobre $M(v(B))$, j se estende a uma k-imersão j' de E em Ω ([Lan02] pág.233 Teorema 2.8) que sobre M coincide com u^{-1} e sobre $k(v(B))$ coincide com v^{-1}, ou seja, j' dá a equivalência entre C e $C(\phi = j' \circ v) = (L(\phi(L')), \mathrm{id}_L, \phi)$, onde $\phi : L' \to j'(M')$ é um $k(B)$-isomorfismo. Resumindo, temos o seguinte diagrama



Para a segunda parte, considere o seguinte diagrama



Para que duas extensões compostas $C(\phi)$ e $C(\psi)$ sejam equivalentes é necessário e suficiente que exista um k-isomorfismo h entre $L(\phi(L'))$ e $L(\psi(L'))$ que é identidade sobre L e tal que $\psi = h \circ \phi$. Mas ψ e ϕ são identidade sobre $k(B)$ e h é identidade sobre L, ou seja, h já é um $L(B)$-isomorfismo, assim, como Ω é algebricamente fechado e $\Omega/L(\phi(L'))$ é algébrico, segue que h se estende a um $L(B)$-automorfismo f de Ω tal que $\psi = f \circ \phi$ (pelo mesmo resultado do Lang citado acima). Agora, se existe tal f com as propriedades acima, então restringindo f a $L(\phi(L'))$ obtemos h.

■

Proposição 1.3.22. *Sejam L e L' duas extensões de k, B uma base de transcendência de L' sobre k. Então, em $L(B) \otimes_{k(B)} L'$, todo ideal primo é maximal e existe uma correspondência biunívoca entre os ideais primos de $L(B) \otimes_{k(B)} L'$ e os tipos de extensões compostas de L e L'.*

Demonstração: Seja $C = (E, u, v)$ uma extensão composta de L e L'. Defina $g : L \otimes_k L' \to E$ por $g(a \otimes b) = u(a)v(b)$. Escreva $\ker(g) = p$, que é um ideal primo de $L \otimes_k L'$. Como L e L' mergulham em E, então g define um isomorfismo $\widetilde{g}$ de $F \stackrel{\text{def}}{=} \text{Frac}((L \otimes_k L')/p)$ sobre E tal que, denotando por $\widetilde{u}, \widetilde{v}$ os homomorfismos naturais de L, L' em F respectivamente, temos que $u = g' \circ \widetilde{u}$ e $v = g' \circ \widetilde{v}$. Ou seja, C é equivalente à extensão composta $(F, \widetilde{u}, \widetilde{v})$.

Sejam p um ideal primo de $L \otimes_k L'$, $F \stackrel{\text{def}}{=} \text{Frac}((L \otimes_k L')/p)$ e $\widetilde{u}, \widetilde{v}$ os homomorfismos naturais de L, L' em F respectivamente. Para que $(F, \widetilde{u}, \widetilde{v})$ seja uma extensão composta, isto é, que $\widetilde{u}(L)$ e $\widetilde{v}(L')$ sejam algebricamente disjuntos, é necessário e suficiente que os monômios com relação aos elementos de $\widetilde{v}(B)$ sejam linearmente independentes sobre $\widetilde{u}(L)$ (elementos algébricos são algebricamente dependentes), ou seja, que $p \cap (L \otimes_k k[B]) = (0)$. Como $A = L \otimes_k L' \cong (L \otimes_k k(B)) \otimes_{k(B)} L'$, podemos mergulhar $L \otimes_k L'$ em $A' = L(B) \otimes_{k(B)} L'$, pois $L \otimes_k k(B)$ mergulha em $L(B)$ e também temos que $A' = S^{-1}(A)$ onde $S = (L[B]) \setminus \{0\}$. Com isso, temos uma correspondência biunívoca

entre os ideais primos $p' \subset A'$ e os ideais primos $p \subset A$ tais que $p \cap S = \emptyset$. Com isso, a condição $p \cap (L \otimes_k k[B]) = (0)$ é satisfeita e obtemos a correspondência desejada.

Para finalizar, como $L'/k(B)$ é algébrica, temos que

$$A' = L(B) \otimes_{k(B)} \varinjlim(L'_i) \cong \varinjlim(L(B) \otimes_{k(B)} L'_i) = \varinjlim(A'_i),$$

onde os L'_i's são extensões finitas sobre $k(B)$ contidas em L'. Note que os A'_i's ainda são finitos sobre $L(B)$ pois $\dim_{L(B)}(L(B) \otimes_{k(B)} L'_i) = \dim_{k(B)} L'_i$. Ou seja, temos que $A' = \bigcup_i A'_i$ é uma união de subálgebras de posto finito em $L(B)$. Se p' é um ideal primo de A' então $A'/p' = \cup_i (A'_i/p' \cap A'_i)$ é também uma união de álgebras de posto finito sobre $L(B)$. Porém, uma álgebra de posto finito sobre um corpo que não possui divisores de zero é um corpo (cada A'_i é artiniano e portanto $p' \cap A'_i$ é maximal) e o mesmo vale para A'/p'.

■

Lema 1.3.23. *Sejam L/k uma extensão primária e $B = \{X_i; i \in I\}$, com os X_i's indeterminadas. Então, $L(B)/k(B)$ é uma extensão primária.*

Demonstração: Precisamos mostrar que se $z \in L(B)$ e $a_j \in k(B)$, com $1 \leq j \leq n$, são tais que $z^n + \sum_{j=1}^{n} a_j z^{n-j} = 0$, então podemos encontrar um inteiro $d \geq 0$ tal que $z^{p^d} = u \in k(B)$. Porém, a expressão de z nos a_j's não envolve infinitos X_i's, e portanto, é suficiente provar o lema quando I é finito. Mais ainda, podemos supor que $I = \{1\}$, ou seja, temos apenas X (como é finito, podemos adicionar os X's um por um).

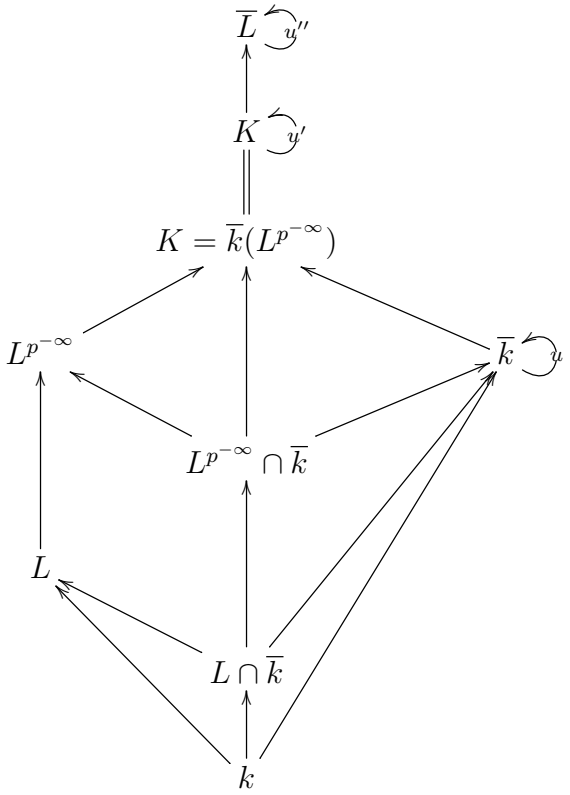
Seja $d \geq 0$ um inteiro tal que $z^{p^d} = u$ é algébrico separável sobre $k(X)$ e suponha que $u \notin k(X)$. Podemos escrever $u = P(X)/Q(X)$ onde $(P, Q) = 1$ e Q é mônico. Seja F o subconjunto de L formado pelos coeficientes de P e Q. Podemos considerar uma derivação não-nula D de $k(F) \neq k$, pois caso contrário, como $k(F)/k$ é finitamente gerado, ele seria algébrico separável sobre k ([Liu02] Lema 1.13(c) pág.214 ou [Mat80] Teorema 59(iii) pág.191), o que iria contradizer o fato de que L é primário sobre k.

A derivação D se estende a uma derivação de $k(F)(X)$, também denotada por D, nula sobre X e portanto sobre $k(X)$. Porém, como u é algébrico separável sobre $k(X)$, teremos $Du = 0$ (como antes) e portanto $D(P)Q - PD(Q) = 0$. Como $DX = 0$, $D(P)$ e $D(Q)$ são obtidos aplicando D nos coeficientes de P e Q, mas Q é mônico, o que mostra que $D(Q)$ é de grau estritamente menor do que Q. Como $D(P)Q - PD(Q) = 0$, temos que Q divide $PD(Q)$ e consequentemente $Q \mid D(Q)$ pois $(P, Q) = 1$. Portanto, $D(Q) = 0$ por causa do grau, implicando que $D(P) = 0$. Como D é aplicado apenas nos coeficientes de P e Q, obtemos que D restrito a F é nulo, o que é uma contradição. Isso mostra que $u \in k(X)$.

■

Lema 1.3.24. *Sejam L/k uma extensão de corpos, $\overline{L}$ um fecho algébrico de L e $\overline{k}$ o fecho algébrico de k em $\overline{L}$. Então, todo k-automorfismo u de $\overline{k}$ que restrito a $L \cap \overline{k}$ é identidade*[3]*, se estende a um L-automorfismo de $\overline{L}$.*

Demonstração: Seja $\{x_i\}_i$ uma base de $L^{p^{-\infty}}$ sobre $L^{p^{-\infty}} \cap \overline{k}$. Temos o seguinte diagrama:



Vamos mostrar que $L^{p^{-\infty}}$ e $\overline{k}$ são linearmente disjuntos sobre $L^{p^{-\infty}} \cap \overline{k}$. Se $L^{p^{-\infty}}$ e $\overline{k}$ não são linearmente disjuntos, existe uma relação linear minimal com coeficientes em $\overline{k}$, a dizer, $\sum a_i x_i = 0$, onde podemos escolher um dos a_i's igual a 1. Se v é um L-automorfismo qualquer de $\overline{L}$, temos $v(x_i) = x_i$ (pois $x_i \in L^{p^{-\infty}}$ o que implica que $x_i^{p^d} \in L$ para algum $d \geq 0$) e obtemos a relação $\sum v(a_i)x_i = 0$. Subtraindo as duas relações, obtemos $\sum (v(a_i) - a_i)x_i = 0$ que envolve um elemento a menos pois temos um $a_i = 1$ e portanto, pela minimalidade assumida, $v(a_i) = a_i$ para todo i. Isso ocorre para todo L-automorfismo v, então, necessariamente temos que $a_i \in L^{p^{-\infty}} \cap \overline{k}$, para todo i. Portanto, os x_i's não são l.i. sobre $L^{p^{-\infty}} \cap \overline{k}$, que é uma contradição.

Seja u como no enunciado. Note que se $x \in L^{p^{-\infty}} \cap \overline{k}$, então $x^{p^d} \in L \cap \overline{k}$ e consequentemente x^{p^d} é invariante por u e com isso x. Desse modo, u é a identidade sobre $L^{p^{-\infty}} \cap \overline{k}$. Como isso ocorre e $L^{p^{-\infty}}$ e $\overline{k}$ são linearmente disjuntos sobre $L^{p^{-\infty}} \cap \overline{k}$,

[3] quando L/k é primária, essa condição sempre ocorre.

podemos estender u de maneira única a um $L^{p^{-\infty}}$-automorfismo u' de $\overline{k}(L^{p^{-\infty}})$. Como $\overline{L}$ é um fecho algébrico de $\overline{k}(L^{p^{-\infty}})$, u' se estende a um L-automorfismo u'' de $\overline{L}$ ([Lan02] pág.233 Teorema 2.8), como queríamos.

■

De posse desses quatro resultados, podemos demonstrar o seguinte teorema, que tem um papel fundamental nesse trabalho.

Teorema 1.3.25. *Seja L/k uma extensão primária de corpos. Se L'/k é uma extensão de corpos qualquer, então existe apenas um tipo de extensão composta de L e L'. Além disso, todo divisor de zero em $L \otimes_k L'$ é nilpotente.*

Demonstração: Seja B uma base de transcendência de L' sobre k e seja $\Omega = \overline{L(B)}$. Pela Proposição 1.3.21 é suficiente mostrar que $C(\phi)$ e $C(\phi')$ são equivalentes, ou seja, que a $k(B)$-imersão $\psi = \phi' \circ \phi^{-1}$ de $\phi(L')$ em Ω se estende a um $L(B)$-automorfismo de Ω. Mas, $\phi(L')$ é algébrico sobre $k(B)$ e portanto ([Lan02] pág.233 Teorema 2.8) ψ se estende para um $k(B)$-automorfismo ψ' de $\overline{k(B)}$.

Pelo Lema 1.3.23, $L(B)/k(B)$ é primária, ou seja, $L(B) \cap \overline{k(B)}$ é puramente inseparável sobre $k(B)$ (por definição) e portanto é invariante por ψ'. Pelo Lema 1.3.24, o $k(B)$-automorfismo ψ' de $\overline{k(B)}$ se estende a um $L(B)$-automorfismo de $\Omega = \overline{L(B)}$. Portanto, existe apenas um tipo de extensão composta de L e L'.

Pela Proposição 1.3.22, $A' \stackrel{def}{=} L(B) \otimes_{k(B)} L'$ tem um único ideal primo que é maximal e assim, todo divisor de zero é nilpotente em A. Como $L \otimes_k k(B) \hookrightarrow L(B)$, temos que $L \otimes_k L' \cong (L \otimes_k k(B)) \otimes_{k(B)} L'$ pode ser identificado com um subanel de A'. Isso encerra a prova.

■

Observação 1.3.26. O Teorema 1.3.25 nos diz que $\mathrm{Spec}\,(L \otimes_k L')$ é irredutível, ou seja, L/k primária implica que L é geometricamente irredutível.

Lembrando que integral significa reduzido e irredutível temos a seguinte

Definição 1.3.27. *Seja S uma k-álgebra. S é geometricamente integral sobre k se, e somente se, S é geometricamente irredutível e geometricamente reduzida sobre k. Nesse caso, $S \otimes_k L$ é um domínio para qualquer extensão L/k.*

Se fortalecermos a hipótese do Teorema 1.3.25 dizendo que L/k também é separável, obtemos outro importante resultado. Note que o Lema 1.3.9 e a Proposição 1.3.7 nos dão condições em que a extensão L/k é separável e portanto é uma hipótese verificável em vários casos.

Teorema 1.3.28. *Se L/k é uma extensão regular então L é geometricamente integral sobre k.*

Demonstração: Como L/k é primária, temos que L é geometricamente irredutível pelo Teorema 1.3.25. Como L/k é separável, L é geometricamente reduzida pelo Lema 1.3.17.

■

Destacamos dois casos importantes do Teorema 1.3.28:

Corolário 1.3.29. *Seja L/k uma extensão de corpos.*

1. *Se $k = \overline{k}$, então L é geometricamente integral sobre k.*
2. *Se k é perfeito e se L/k é primária, então L é geometricamente integral sobre k.*

Demonstração:

1. Se $k = \overline{k}$, então k é algebricamente fechado em L. Pelo Lema 1.3.9, L/k é separável e portanto regular.
2. Se k é perfeito então L/k é separável pelo Lema 1.3.9. Como L/k é primária, então L/k é regular.

■

O lema a seguir nos dá um resultado interessante com relação a álgebras com um único primo minimal.

Lema 1.3.30. *Seja k um corpo separavelmente algebricamente fechado. Sejam R, S duas álgebras que tem um único primo minimal. Então, $R \otimes_k S$ também tem um único primo minimal.*

Demonstração: Inicialmente, faremos uma redução para o caso em que $k = \overline{k}$. Para isso, considere $R \hookrightarrow R \otimes_k \overline{k}$ e vamos mostrar que o morfismo induzido em Spec é uma bijeção que preserva inclusão. Note que se $x \in R \otimes_k \overline{k}$ então existe $n \geq 1$ tal que $x^n \in R$, pois k é separavelmente algebricamente fechado. Note que o morfismo induzido $\phi : \mathrm{Spec}(R \otimes_k \overline{k}) \to \mathrm{Spec}(R)$ é sobrejetor (pois $R \otimes_k \overline{k}/R$ é integral: ver [Mat80] pág.33 Teorema 5). Além disso, ϕ preserva inclusão por definição. Resta mostrar que ϕ é injetor: seja $p, q \in \mathrm{Spec}(R \otimes_k \overline{k})$ e suponha que $p \cap R = q \cap R$. Se $x \in p$ então existe n tal que $x^n \in p \cap R = q \cap R$ e portanto $x \in q$, pois q é primo. Portanto, ϕ é bijeção e preserva inclusão, ou seja, leva primo minimal em primo minimal. O mesmo vale para $S \hookrightarrow S \otimes_k \overline{k}$ e $R \otimes_k S \hookrightarrow (R \otimes_k S) \otimes_k \overline{k} = R \otimes_k \overline{k} \otimes S \otimes_k \overline{k}$. Com isso, temos a redução desejada e podemos supor que k é algebricamente fechado.

Podemos também trocar R e S por suas reduções (de fato, $\mathrm{Spec}(R) \cong \mathrm{Spec}(R_{\mathrm{red}})$, pois temos uma correspondência biunívoca entre os primos de $R/\sqrt{0}$ e os primos de R que contém $\sqrt{0}$) e assim assumir que R e S são domínios. Portanto, $R \otimes_k S$ é reduzido pelo Lema 1.3.19. Portanto, seu Spec é redutível se, e somente se, contém algum divisor de zero não nulo. Pelo Lema 1.3.13, podemos finalmente reduzir ao caso em que R e S são domínios de tipo finito sobre um corpo algebricamente fechado k.

Para finalizar, precisamos mostrar que $R \otimes_k S$ é domínio. Suponha que $f, g \in R \otimes_k S$ são tais que $fg = 0$. Escreva $f = \sum a_i \otimes b_i$ e $g = \sum c_i \otimes d_i$ onde os b_i's são l.i. sobre k, assim como os d_i's. Para cada ideal maximal m de R faça a redução módulo m. Como $k = \overline{k}$, pelo Nullstellensatz, $R/m \cong k$, ou seja, $(R/m) \otimes_k S \cong S$ e assim $(\sum \overline{a_i} \otimes b_i)(\sum \overline{c_i} \otimes d_i)$ está em S, onde $\overline{a_i}, \overline{c_i} \in k$ para todo i.

Como S é domínio, temos que $\sum \overline{a_i} \otimes b_i = 0$ ou $\sum \overline{c_i} \otimes d_i = 0$, ou seja, $a_i \in m$ para todo i ou $c_i \in m$ para todo i.

Portanto,

$$\mathrm{spm}(A) = V(a_1, \cdots, a_n) \cup V(c_1, \cdots, c_n),$$

onde spm é o conjunto dos ideais maximais de A. Mas, $\mathrm{spm}(A)$ é irredutível (ver [Milb] pág.48 Proposição 2.19) e assim $\mathrm{spm}(A)$ é igual a $V(a_1, \cdots, a_n)$ ou $V(c_1, \cdots, c_n)$. Se $\mathrm{spm}(A) = V(a_1, \cdots, a_n)$ ocorre, então $I(V(a_1, \cdots, a_n)) = \sqrt{(a_1, \cdots, a_n)}$ pelo Nullstellensatz. Por outro lado, $I(\mathrm{spm}(A)) = (0)$. Portanto, $f = 0$. O outro caso é análogo. ■

Infelizmente, no caso de geometricamente irredutível não teremos diretamente um resultado como o Teorema 1.3.18, mas temos o seguinte:

Teorema 1.3.31. *Sejam k um corpo e R uma k-álgebra. São equivalentes:*

(1) $\mathrm{Spec}(R \otimes_k L)$ *é irredutível para toda extensão de corpos L/k;*

(2) $\mathrm{Spec}(R \otimes_k L)$ *é irredutível para toda extensão separável finita L/k.*

Demonstração: Precisamos provar que (2) $\Rightarrow$ (1). Pelo mesmo argumento no início da demonstração do Lema 1.3.30, podemos trocar R por $(R \otimes_k k^{p^{-\infty}})_{\mathrm{red}}$ e k por $k^{p^{-\infty}}$, ou seja, podemos supor que k é perfeito. Portanto, pelo Teorema 1.3.18 podemos assumir que R é geometricamente reduzido.

Então, suponha que R é geometricamente reduzido sobre k. Nesse caso, para qualquer extensão L/k, a irredutibilidade de $\mathrm{Spec}(R \otimes_k L)$ é equivalente a $R \otimes_k L$ ser um domínio.

Seja $\overline{k}$ um fecho algébrico separável de k. Pelo Lema 1.3.13, temos que (2) é equivalente a $R \otimes_k \overline{k}$ ser um domínio. Para qualquer extensão de corpos L/k, existe uma extensão de corpos $\overline{L}/k$ que contém $\overline{k}$ e L. Então, pelo Lema 1.3.30, temos que

$R \otimes_k \overline{L} \cong (R \otimes_k \overline{k}) \otimes_{\overline{k}} \overline{L}$ é um domínio. Logo, $R \otimes_k L$ é domínio, pois R é plano sobre k e $L \hookrightarrow \overline{L}$.

■

1.3.4 Variedades geometricamente integrais

Vamos estudar o caso em que L é o corpo de funções de uma variedade algébrica. Nesta subseção, veremos quando uma variedade algébrica, mais geralmente um esquema, é geometricamente reduzido e irredutível, onde grande parte dos resultados serão consequências do caso de álgebras . Primeiro, vejamos algumas definições e exemplos. Os principais resultados dessa subseção são os Teoremas 1.3.36, 1.3.38 e 1.3.42.

Definição 1.3.32. *Seja X uma variedade algébrica sobre um corpo k. Dizemos que X é geometricamente reduzido* (*resp. integral, irredutível*) *sobre k se $X \times_k L$ é reduzido* (*resp. integral, irredutível*) *para toda extensão de corpos L/k.*

Observação 1.3.33. A definição anterior pode ser dada para esquemas. Por isso, quase todos os resultados que seguem serão provados para um esquema qualquer.

O exemplo a seguir mostra que uma variedade algébrica integral nem sempre é geometricamente integral.

Exemplo 1.3.34. Considere $X = \operatorname{Spec} \mathbb{C}[x]$ como variedade sobre $\operatorname{Spec} \mathbb{R}$. Temos que X é integral, pois $\mathbb{C}[x]$ é domínio, porém X não é geometricamente integral. De fato

$$X_{\mathbb{C}} = X \times_{\operatorname{Spec} \mathbb{R}} \operatorname{Spec} \mathbb{C} \cong \operatorname{Spec}(\mathbb{C}[x] \otimes_{\mathbb{R}} \mathbb{C}).$$

Mas note que

$$\mathbb{C}[x] \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[x] \otimes_{\mathbb{R}} \left(\frac{\mathbb{R}[y]}{(y^2+1)} \right) \cong \frac{\mathbb{C}[x,y]}{(y^2+1)} \cong \frac{\mathbb{C}[x,y]}{(y+i)(y-i)} \overset{\text{TCR}}{\cong} \mathbb{C}[x] \times \mathbb{C}[x],$$

onde no último isomorfismo usamos o Teorema Chinês dos Restos. Isso mostra que $X_{\mathbb{C}}$ possui duas componentes conexas e portanto não é integral.

Temos ainda mais dois exemplos:

Exemplo 1.3.35.

- Sejam $k = \mathbb{F}_p$, com p primo, e $K = \mathbb{F}_p(x)$ uma extensão puramente transcendente de k. Considere a variedade $X = \operatorname{Spec}(K[T]/(T^p - x))$ (que é reduzida). Seja k' uma extensão de k tal que k' contém uma p-ésima raiz de x. Então, $T^p - x = (T - x^{1/p})^p$ em $k'[T]$ e portanto $X_{k'}$ não é reduzido, pois $k'[T]/(T^p - x)$ contém, por exemplo, $\overline{T - p^{1/p}}$ que não é nulo, mas sua p-ésima potência é.

- Considere $X = \operatorname{Spec}(\mathbb{Q}(i))$ como variedade sobre $\operatorname{Spec}\mathbb{Q}$. Temos que X é uma variedade integral mas não geometricamente integral. Se fizermos uma mudança de base por $\mathbb{C}$, ou seja, por $\operatorname{Spec}\mathbb{C}$, temos que $X_{\mathbb{C}} = \operatorname{Spec}(\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{C})$. Porém, $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$ pelo Teorema Chinês dos Restos, tornando $X_{\mathbb{C}}$ uma união disjunta de duas cópias de $\operatorname{Spec}\mathbb{C}$.

Como no caso de álgebras, para verificar se um esquema X é geometricamente irredutível ou reduzido, não é necessário verificar que X_L é irredutível ou reduzido para toda extensão L/k, como mostram os próximos dois teoremas.

Teorema 1.3.36. *Sejam k um corpo e X um k-esquema. Então são equivalentes:*

(1) X é geometricamente reduzido;

(2) X_L é reduzido para toda extensão de corpos L/k;

(3) X_L é reduzido para toda extensão finita puramente inseparável L/k;

(4) $X_{k^{1/p}}$ é reduzido;

(5) $X_{k^{p^{-\infty}}}$ é reduzido;

(6) $X_{\overline{k}}$ é reduzido;

(7) para todo aberto afim $U \subset X$, a k-álgebra $\mathcal{O}_X(U)$ é geometricamente reduzida.

Demonstração: Por definição (1) $\Leftrightarrow$ (2).

Vamos provar que (2) $\Rightarrow$ (7). Sejam $U \subset X$ um aberto afim e L/k uma extensão de corpos qualquer. Então, X_L é reduzido e consequentemente $U_L = \operatorname{Spec}(\mathcal{O}_X(U) \otimes_k L)$ é reduzido. Portanto, $\mathcal{O}_X(U) \otimes_k L$ é reduzido e temos que $\mathcal{O}_X(U)$ é geometricamente reduzido.

Vamos provar que (7) $\Rightarrow$ (1). Seja L/k uma extensão de corpos qualquer. Como X é a colagem de esquemas afins, temos que a mudança de base X_L é obtida por colagem dos abertos $U_L = \operatorname{Spec}(\mathcal{O}_X(U) \otimes_k L)$, onde $U \subset X$ é aberto afim, e portanto, X_L é reduzido.

Assim, temos (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (7). Agora, suponha (6). Por definição, $X_{\overline{k}}$ reduzido é equivalente a $\mathcal{O}_X(U) \otimes_k \overline{k}$ ser reduzido para todo aberto afim U de X. Pelo Teorema 1.3.18, isso é equivalente a $\mathcal{O}_X(U)$ ser geometricamente reduzido, obtemos o item (7). Portanto, (6) $\Leftrightarrow$ (7). Os outros itens são provados do mesmo modo.

■

Antes do próximo teorema, vejamos uma primeira consequência da definição de geometricamente irredutível.

Lema 1.3.37. *Seja X um esquema sobre um corpo k. Seja L/k uma extensão de corpos qualquer. Então, X é geometricamente irredutível sobre k se, e somente se, X_L é geometricamente irredutível sobre L.*

Demonstração: Se X é geometricamente irredutível sobre k então é claro que X_L é geometricamente irredutível sobre L. Para qualquer extensão de corpos k'/k existe uma extensão de corpos L'/k contendo L e k'. Note que $X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(L') \to X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k')$ é um morfismo de esquemas sobrejetor, pois $\mathrm{Spec}(L') \to \mathrm{Spec}(k')$ é sobrejetor e fazemos uma mudança de base sobre $\mathrm{Spec}(k)$ em $\mathrm{id} : X \to X$ (ver [Sta] Lema 24.11.4 pág.1418). Desse modo, temos que a sobrejetividade de

$$X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(L') \cong (X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(L)) \times_{\mathrm{Spec}(L)} \mathrm{Spec}(L') \twoheadrightarrow X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k')$$

implica que $X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k')$ é irredutível pois $(X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(L)) \times_{\mathrm{Spec}(L)} \mathrm{Spec}(L')$ é irredutível por hipótese e portanto X é geometricamente irredutível sobre k.

■

Note que o Lema 1.3.37 implica em um resultado equivalente no caso de álgebras. De fato, um esquema afim $\mathrm{Spec}(A)$ é geometricamente irredutível se, e somente se, A é geometricamente irredutível. O próximo teorema nos dará alguns métodos de verificar se um esquema X é geometricamente irredutível.

Teorema 1.3.38. *Sejam k um corpo e X um k-esquema. Então são equivalentes:*

(1) X é geometricamente irredutível;

(2) para qualquer aberto afim $U \subset X$, a k-álgebra $\mathcal{O}_X(U)$ é geometricamente irredutível sobre k;

(3) X é irredutível e existe uma cobertura aberta afim $X = \bigcup U_i$ tal que cada k-álgebra $\mathcal{O}_X(U_i)$ é geometricamente irredutível;

(4) existe uma cobertura aberta $X = \bigcup_{i \in I} X_i$ tal que X_i é geometricamente irredutível para cada i e tal que $X_i \cap X_j \neq \emptyset$ para todo $i, j \in I$.

Além disso, se X é geometricamente irredutível então também são todos os subesquemas abertos de X.

Demonstração: Vamos fazer algumas observações. Primeiro, já vimos que um esquema afim $\mathrm{Spec}(A)$ é geometricamente irredutível se, e somente se, A é geometricamente irredutível. Se um esquema X é irredutível, então todo subesquema aberto de X é irredutível e qualquer dois abertos não vazios tem interseção não vazia (basta lembrar que se X é irredutível, então $X = \overline{\{\xi\}}$, onde ξ é o único ponto genérico de

X (ver [Liu02] Definição 4-10 pág.63), e isso implica que ξ é um elemento (denso) contido em todo aberto U não vazio). Além disso, suponha que temos $X = \bigcup U_i$ uma união de abertos afim e suponha que todo aberto afim é irredutível; se temos $U_i \cap U_j = \emptyset$ então $U_i \sqcup U_j$ é um aberto afim que é irredutível por hipótese, o que é um absurdo. Portanto, (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4). Vamos mostrar que (4) $\Rightarrow$ (1). Bem, seja L/k uma extensão. Temos que (4) vale para X_L. Suponha que $X_L = B \cup B'$ é uma união disjunta de dois subsquemas fechados. Desse modo, podemos escrever cada $(X_i)_L = (B \cap (X_i)_L) \cup (B' \cap (X_i)_L)$. Porém, $(X_i)_L$ é irredutível e assim $(X_i)_L \subset B$ ou $(X_i)_L \subset B'$. Suponha que $(X_i)_L \subset B$ e que $(X_i)_L \cap (X_j)_L \neq \emptyset$. Então, como $(X_j)_L = (B \cap (X_j)_L) \cup (B' \cap (X_j)_L)$ e $(X_j)_L$ é irredutível, temos que $(X_j)_L \subset B$, pois $(X_i)_L \cap (X_j)_L \neq \emptyset$ e $(X_i)_L \subset B$. Procedendo desta forma, obtemos que $X_L = B$ é irredutível. O caso $(X_i)_L \subset B'$ é análogo.

■

O teorema 1.3.38 ainda pode ser melhorado em alguns casos. O primeiro é o:

Teorema 1.3.39. *Seja X um esquema sobre um corpo separavelmente algebricamente fechado sobre k. Se X é irredutível então X é geometricamente irredutível sobre k.*

Demonstração: Por um argumento semelhante ao usado na demonstração do Teorema 1.3.38, X irredutível é equivalente a todo aberto afim U ser irredutível. Pelo Lema 1.3.30, $\mathcal{O}_X(U) \otimes_k L$ é irredutível para toda extensão L/k .

■

Temos ainda mais dois casos para analisar:

Corolário 1.3.40. *Seja X um esquema. X é geometricamente irredutível sobre k se, e somente se, X_{k^s} é irredutível se, e somente se, X_L é irredutível para toda extensão finita separável L/k.*

Demonstração: Pelo Lema 1.3.37,X_{k^s} é geometricamente irredutível sobre k^s se, e somente se, X é geometricamente irredutível sobre k. Note que k^s é separavelmente algebricamente fechado. Por definição, X geometricamente irredutível sobre k implica que X_{k^s} é irredutível. Pelo Teorema 1.3.39, temos que se X_{k^s} é irredutível então X_{k^s} é geometricamente irredutível sobre k^s.

Além disso, pelos Teoremas 1.3.31 e 1.3.38, também podemos concluir que X é geometricamente irredutível se, e somente se, X_L é irredutível para toda extensão finita separável L/k.

■

Observação 1.3.41. Pelo Corolário 1.3.40 e o Teorema 1.3.36 restringimos a verificação de que um esquema X é geometricamente reduzido e irredutível somente sobre as extensões $\overline{k}/k$ e k^s/k, respectivamente. Então temos:

- X é geometricamente reduzido sobre k se, e somente se, $X \otimes_K \overline{k}$ é reduzido;
- X é geometricamente irredutível sobre k se, e somente se, $X \otimes_k k^s$ é irredutível.

Quando k é perfeito, $\overline{k} = k^s$ e portanto precisamos apenas de uma verificação.

O teorema a seguir também é muito importante e terá conexão com outros resultados como veremos na Observação 1.3.44.

Teorema 1.3.42. *Seja X uma variedade algébrica integral sobre k com corpo de funções $k(X) \stackrel{def}{=} \mathcal{O}_{X,\xi}$, onde ξ é o ponto genérico de X.*

(*a*) *X é geometricamente integral sobre k se, e somente se, $k(X)$ e $\overline{k}$ são linearmente disjuntos sobre k. Nesse caso, $k(X_{\overline{k}}) = k(X) \otimes_k \overline{k}$.*

(*b*) *X é geometricamente irredutível sobre k se, e somente se, $k(X) \cap k^s = k$.*

Demonstração:

(a) Suponha que $k(X)$ e $\overline{k}$ são linearmente disjuntos sobre k e vamos mostrar que $X_{\overline{k}}$ é integral, ou seja, que X é geometricamente integral sobre k. Isso é equivalente a mostrar que $\mathcal{O}_{X_{\overline{k}}}(U_{\overline{k}})$ é domínio integral para todo aberto afim U de X. Para qualquer aberto afim U de X temos

$$\mathcal{O}_{X_{\overline{k}}}(U_{\overline{k}}) = \mathcal{O}_X(U) \otimes_k \overline{k} \subset k(X) \otimes_k \overline{k},$$

ou seja, $\mathcal{O}_{X_{\overline{k}}}(U_{\overline{k}})$ é domínio integral. Por outro lado, suponha que X é geometricamente integral (ou seja, $X_{\overline{k}}$ é integral) e vamos mostrar que $k(X)$ e $\overline{k}$ são linearmente disjuntos sobre k. Seja $U = \mathrm{Spec}(A)$ aberto afim de X, onde A é um k-domínio integral. Temos que $k(X) \otimes_k \overline{k}$ é um domínio, pois é uma localização de $A \otimes_k \overline{k}$. Além disso, $k(X) \otimes_k \overline{k}$ é integral sobre $k(X)$ e portanto, $k(X) \otimes_k \overline{k}$ é corpo, pois $k(X)$ é corpo (ver [Mat89] pág.66 Lema 1). Isso nos diz que $k(X)$ e $\overline{k}$ são linearmente disjuntos sobre k.[4] Resta verificar que

$$\overline{k}(X_{\overline{k}}) = \mathrm{Frac}(A \otimes_k \overline{k}) \cong \mathrm{Frac}(A) \otimes_k \overline{k} \cong k(X) \otimes_k \overline{k}.$$

Mas, $A \otimes_k \overline{k} \subset \mathrm{Frac}(A) \otimes_k \overline{k} \subset \mathrm{Frac}(A \otimes_k \overline{k})$ e já vimos que $\mathrm{Frac}(A) \otimes_k \overline{k}$ é corpo, portanto, temos a igualdade.

[4] a aplicação $k(X) \otimes_k \overline{k} \to k(X)(\overline{k})$ é sempre injetora, pois é não-nula e $k(X) \otimes_k \overline{k}$ é corpo, onde $k(X)(\overline{k})$ é o menor corpo gerado por $k(X)$ e $\overline{k}$.

(b) Escreva $K \stackrel{def}{=} k(X) \cap k^s$. Suponha que X é geometricamente irredutível e vamos mostrar que $K = k$. Então, X_{k^s} é irredutível. Pelo Lema 1.3.16 ele também é reduzido, logo integral. Analogamente ao feito na letra (a), podemos mostrar que $k^s(X_{k^s}) = k(X) \otimes_k k^s$. Observe que $k(X) \otimes_k k^s \supset K \otimes_k K$, que é portanto um domínio. Isso implica que $K = k$. De fato, suponha que $k \subset K$ propriamente. Então existe uma extensão separável finita k'/k tal que $k \subset k' \subset k(X) \cap k^s$. Mas, $k' \otimes_k k' \cong k'[T]/(p(T))$, onde $p(T)$ é irredutível sobre $k[T]$, mas tem raiz em k', o que é absurdo. Agora, suponha que $K = k$ e vamos mostrar que X é geometricamente irredutível. Para isso, é suficiente mostrar que $k(X) \otimes_k K'$ é domínio integral para qualquer extensão separável finita K' de k (pelo Corolário 1.3.40 e pois $\mathcal{O}_X(U) \subset k(X)$, para todo aberto afim $U \subset X$). Temos que $K' = k(\theta) = k[T]/(P(T))$, onde $p(T)$ é o polinômio minimal de θ sobre k. Então,

$$k(X) \otimes_k K' \cong k(X) \otimes_k (k[T]/(P(T))) \cong k(X)[T]/(P(T)),$$

ou seja, para mostrar que $k(X) \otimes_k K'$ é um domínio basta mostrar que $P(T)$ é irredutível em $k(X)[T]$. Seja $Q(T) \in k(X)[T]$ um polinômio mônico que divide $P(T)$. Como $P(T)$ se fatora sobre k^s então $Q(T) \in k^s[T]$. Assim, $Q(T) \in (k(X) \cap k^s)[T] = k[T]$ e consequentemente $Q = 1$ ou $Q = P$. Portanto, $P(T)$ é irredutível em $k(X)[T]$.

■

Temos ainda outro critério para decidir quando uma variedade algébrica integral X é geometricamente reduzida.

Proposição 1.3.43 ([Liu02] pág.91)**.** *Seja X uma variedade algébrica integral sobre k. Então, X é geometricamente reduzido se, e somente se, $k(X)$ é uma extensão finita separável de uma extensão puramente transcendente $k(T_1, \ldots, T_d)$.*

Concluímos o capítulo com a seguinte:

Observação 1.3.44. Seja X uma variedade algébrica geometricamente integral e seja L o corpo de funções de X . Pelo Teorema 1.3.42, isso é equivalente a L e $\overline{k}$ serem linearmente disjuntos. Pelo Teorema 1.3.8, essa condição é ainda equivalente a L/k ser regular. Com isso, pelo Teorema 1.3.28, segue que $L \otimes_k L'$ é domínio para qualquer extensão de corpos L'/k. Em particular, $L \otimes_k L$ é domínio e k é algebricamente fechado em L.

Quando o corpo k é perfeito, pelo Teorema 1.3.42, verificar que X é geometricamente integral é equivalente a verificar se X é geometricamente irredutível. Pelo Lema 1.3.9, L/k é separável e assim, pelo Lema 1.3.17, isso é equivalente a L ser geometricamente reduzido.

Capítulo

2

A conjectura de Makar-Limanov

Neste capítulo, estenderemos um pouco mais a discussão sobre a conjectura de Makar-Limanov e a conjectura GA. Inicialmente, mostraremos alguns resultados já conhecidos. Em seguida, discutiremos sobre as hipóteses da conjectura de Makar-Limanov e sobre os resultados dos próximos capítulos.

2.1 Resultados conhecidos

Nesta seção apresentaremos uma cronologia de artigos sobre a conjectura de Makar-Limanov e a conjectura GA, destacando em cada artigo alguns dos principais resultados. Vale notar que não citaremos os artigos sobre a conjectura de Lichtman, apesar de que alguns dos trabalhos abaixo também tratam dessa conjectura.

Sobre a conjectura de Makar-Limanov e a conjectura GA temos os seguintes resultados:

• **Em** 1983, L. Makar-Limanov em [ML83] prova o já citado resultado sobre o corpo skew de frações da álgebra de Weyl D_1. Além disso, é levantada uma questão sobre as possíveis dimensões de Gelfand-Kirillov de subálgebras de D_1.

• **Em** 1984, L. Makar-Limanov em [ML84a] levanta algumas questões sobre a existência de estruturas livres em corpos skew, a dizer, semigrupos livres, grupos livres e álgebras livres de posto 2. Com relação a semigrupos, Makar-Limanov prova que *se k é não-enumerável, então existe um semigrupo livre no corpo skew D, quando D é*

gerado sobre seu centro k por elementos p, q tais que $pq - qp = 1$ (na verdade vale um pouco mais geral esse resultado). Para grupos, ele *provou que quando o corpo skew D tem dimensão finita sobre seu centro k então todo subgrupo normal não central de $D^\times$ (grupo multiplicativo de D) contém um subgrupo livre de posto* 2. Finalmente, para o caso de álgebras, Makar-Limanov prova a existência de *subálgebras livres na álgebra de divisão D (gerada sobre seu centro k por elementos p, q tais que $pq - qp = 1$) e no anel de frações da álgebra de grupo $K[G]$, com G um grupo nilpotente gerado por elementos a, b satisfazendo $aba^{-1}b^{-1} = c \neq 1$ e $aca^{-1}c^{-1} = bcb^{-1}c^{-1} = 1$*, usando a mesma técnica de [ML83]. Nesse artigo ele propõe a Conjectura A.

• **Em** 1984, L. Makar-Limanov em [ML84b] prova que *se G é um grupo nilpotente livre de torsão não-abeliano e F é um corpo então o corpo skew de frações* $\mathrm{Frac}(F[G])$ *do anel de grupo $F[G]$ contém uma subálgebra livre não-comutativa de posto* 2.

• **Em** 1984, A.I. Lichtman em [Lic84] mostrou que em certos casos a conjectura de Makar-Limanov implica na conjectura GA. Temos o seguinte resultado:

Teorema 2.1.1. *Seja $D = \mathrm{Frac}\, R$ com centro k, onde R é um domínio de Ore com uma valorização discreta v. Suponha que elementos a, b geram uma k-subálgebra livre em D. Se $v(a) \geq 1$ e $v(b) \geq 1$, então os elementos $1 + a, 1 + b$ geram o anel de grupo do grupo livre de posto* 2 *em D.*

• **Em** 1986, M. Lorenz em [Lor86] unificou os resultados de Makar-Limanov contidos em [ML83] e [ML84b], melhorando as técnicas apresentadas nesses trabalhos. Ele enunciou o seguinte resultado:

Teorema 2.1.2. *Sejam $L = k(t)$ o corpo de funções racionais sobre o corpo k, $\sigma \in \mathrm{Aut}_k(L)$ de ordem infinita e $L[t; \sigma]$ o anel de polinômios skew. Então, o anel de divisão de frações $D = \mathrm{Frac}(L[t; \sigma])$ contém uma k-subálgebra livre não-comutativa de posto* 2.

• **Em** 1991, L. Makar-Limanov em [ML91] apresenta 2 subálgebras do corpo skew de frações da primeira álgebra de Weyl, uma delas maximal na classe de subálgebras com dimensão de Gelfand-Kirillov finita.

• **Em** 1991, L. Makar-Limanov e P. Malcolmson em [MLM91] provaram que *se L é uma álgebra de Lie não-abeliana sobre um corpo k (chark=0) então o corpo skew de frações da álgebra envelopante de L sobre k contém uma k-álgebra livre não-comutativa quando L é solúvel ou de dimensão finita.* Além disso, eles provaram o seguinte lema:

Lema 2.1.3. *Seja R um domínio com subcorpo primo k_0 (subcorpo gerado por 1_R). Seja C qualquer subcorpo central de R e sejam $y, z \in R$. Então, y e z são livres sobre k_0 se, e somente se, eles são livres sobre C.*

• **Em** 1996, Z. Reichstein em [Rei96] provou o seguinte resultado geral:

Teorema 2.1.4. *Sejam k corpo não-enumerável, $k \subset L$ uma extensão de corpos e A uma k-álgebra associativa. Se $L \otimes_k A$ contém uma k-subálgebra livre não-comutativa, então A também contém.*

Esse resultado tem significante importância nas *conjecturas FOFO*, pois ele responde parte da seguinte conjectura, também proposta por Makar-Limanov e descrita em [Rei96]:

Conjectura C. *Sejam D um corpo skew, k_0 o subcorpo primo de $Z(D)$, k um subcorpo de $Z(D)$ e L uma extensão de k. Se $L \otimes_k D$ contém uma k_0-álgebra livre, então D também contém.*

• **Em** 1996, M. Shirvani e J. Z. Gonçalves em [SG96] provaram o seguinte resultado geral, mas que também depende da não-enumerabilidade do centro da álgebra de divisão:

Teorema 2.1.5. *Seja D uma álgebra de divisão com centro não enumerável k. Se D contém uma k-álgebra livre não-comutativa de posto 2, então D contém uma k-álgebra de grupo do grupo livre de posto 2.*

Portanto, quando o corpo k é não-enumerável, segue que a conjectura de Makar-Limanov implica a conjectura GA. Note que esse resultado, apesar da restrição sobre o centro, não depende da existência de valorizações como no resultado de Lichtman.

• **Em** 1996, L. M. V. Figueiredo, M. Shirvani e J. Z. Gonçalves em [FGS96] provaram o seguinte resultado: *Seja D uma álgebra de divisão com centro k. Então, D contém a k-álgebra de grupo do grupo livre de posto 2 quando D é o anel de frações de um anel de polinômios skew com certas propriedades, ou ele é gerado por um grupo policíclico-por-finito que não é abeliano-por-finito, ou ele é o anel de frações da álgebra envelopante universal (universal enveloping algebra) de uma álgebra de Lie de dimensão finita de característica zero.*

• **Em** 1998, M. Shirvani e J. Z. Gonçalves em [SG98] provam *a existência de álgebras de grupo do grupo livre no anel de divisão de frações de um anel de polinômios*

diferenciais $D[X;\delta]$, onde δ é uma derivação não-nula e D é uma álgebra de divisão (satisfazendo algumas propriedades).

• **Em** 1999, M. Shirvani e J. Z. Gonçalves em [SG99] provam o seguinte resultado: *sejam k corpo e R uma k-álgebra comutativa. Suponha que R é um domínio. Seja $\sigma \neq \mathrm{id}$ um k-automorfismo de R tal que $R^{\langle\sigma\rangle} = k$ e estenda σ para $L = \mathrm{Frac}(R)$. Então,* $\mathrm{Frac}(L[t;\sigma])$ *contém a álgebra de grupo do grupo livre de posto $|k|$.*

• **Em** 2009, A. Smoktunowicz em [Smo09] mostra que a hipótese de não-enumerabilidade do trabalho [Rei96] de Reichstein é essencial (ver Introdução), ou seja, o resultado é falso quando o corpo k é enumerável, sem impor alguma hipótese extra.

Com relação a grupos ordenados, existe um resultado recente e bem geral:

• **Em** 2011, J. Sánchez em [Sán] provou o seguinte: *seja D um corpo skew e $(G,<)$ um grupo ordenado. Então, o corpo skew do anel de grupo $D[G]$ dentro do anel de séries de Malcev-Neumann $D((G;<))$ contém álgebras de grupo do grupo livre não-comutativas sobre seu centro.*

• **Em** 2012, J. Z. Gonçalves e E. Tengan em [GT12] provaram o seguinte resultado: *sejam $k = \bar{k}$ um corpo de característica 0 e L um corpo de funções sobre k com* $\mathrm{trdeg}_k L = 1$. *Seja σ um k-automorfismo de L de ordem infinita. Então o corpo skew de frações de $L[t;\sigma]$ contém a álgebra de grupo $k[F]$ de um grupo livre F de posto 2.*

Quando supomos que uma álgebra de divisão possui uma certa involução, temos alguns resultados interessantes como os dois artigos a seguir:

• **Em** 2012 [SG12], M. Shirvani e J. Z. Gonçalves.

• **Em** 2012 [FGS96], V.O. Ferreira, J. Z. Gonçalves e J. Sánchez.

Dois trabalhos recentes, mas que merecem destaque pelo grau de generalidade e importância são devidos a J.P. Bell e D. Rogalski.

• **Em** [BRb] os autores provam o seguinte: seja L/k extensão de corpos e σ um k-automorfismo de L. Então $L(t;\sigma)$ contém uma k-subálgebra livre de posto 2 quando ou k é não-enumerável ou σ é induzido por um automorfismo de uma variedade quasi-projetiva. No caso de uma k-derivação δ de L, eles obtiveram o mesmo resultado sem hipóteses adicionais sobre k. Interessantes equivalências são obtidas nesses casos, assim como um resultado no caso de extensões de Ore iteradas, como consequência dos resultados anteriores.

• **Em** [BRa] os autores restringem o estudo ao caso onde k é não-enumerável, porém, obtém um resultado bem geral: *seja A um domínio noetheriano que é enumeravelmente gerado sobre $k = \bar{k}$ de característica 0, então ou o anel de divisão de frações de A contém uma k-álgebra livre de posto 2 ou ele é algébrico à esquerda sobre todo subcorpo maximal.* Além disso, eles provam mais alguns resultados, inclusive sobre domínios com dimensão de Gelfand-Kirillov igual a 2.

2.2 Discussão e contra-exemplos I

Nessa seção discutiremos sobre as hipóteses da conjectura de Makar-Limanov.

Primeiramente, note que se uma álgebra de divisão D com centro k contém uma k-subálgebra livre de posto 2 gerada por elementos $a, b \in D$ então D contém uma k-subálgebra livre de posto n para qualquer $n \geq 2$. De fato, podemos por exemplo considerar como geradores $a, ab, ab^2, \ldots, ab^{n-1}$. Na verdade, isso implicitamente aparecerá na demonstração do Teorema 3.3.5 quando considerarmos monômios formados pelos dois candidatos a geradores (e.g., $a = f$ e $b = t(1 - t^{-1})f$). Em [ML84a], quando Makar-Limanov fala sobre a existência de semigrupos, grupos ou álgebras livres de posto 2, ele escreve: "*It is not reasonable a bigger number of generators, because as is well known, every free object mentioned contains the corresponding free object on a countable number of generators.*"

Para continuar, precisaremos de uma definição.

Definição 2.2.1. *Um anel R é chamado anel de Identidade Polinomial (ou anel PI, polynomial identity ring) se para algum $N > 0$, existe um elemento $P \neq 0$ da álgebra livre $\mathbb{Z}\langle X_1, \ldots, X_N\rangle$ sobre $\mathbb{Z}$ tal que para qualquer N-upla $\{a_1, \ldots, a_N\}$ de elementos de R vale $P(a_1, \ldots, a_N) = 0$.*

Exemplo 2.2.2.

1. Quando R é um anel comutativo, quaisquer dois elementos de R satisfazem a identidade polinomial

$$P(X, Y) = XY - YX = 0.$$

2. Qualquer anel de matrizes $M_n(D)$, matrizes $n \times n$ com entradas em um anel de divisão D, é um anel PI. De fato, quaisquer $N = 2n$ matrizes $n \times n$ satisfazem

$$P(X_1, \ldots, X_N) = \sum_{\sigma} \operatorname{sgn}(\sigma) X_{\sigma(1)} \ldots X_{\sigma(N)} = 0,$$

onde a soma é sobre todas as permutações σ de $\{1, \ldots, N\}$. Esse é um importante resultado de Amitsur e Levitzki em [AL50].

Desse modo, nenhuma álgebra de divisão D sobre k que seja PI (para um $N > 0$ fixo) pode conter uma k-subálgebra livre de posto 2. De fato, se isso ocorre, D deveria conter k-subálgebras livres de qualquer posto $n > 2$, inclusive de posto $n = N$, o que seria absurdo, pois sendo D um anel PI esses N geradores deveriam satisfazer uma identidade polinomial. Portanto, uma condição necessária, mas não suficiente, para que uma álgebra de divisão contenha uma subálgebra livre de posto 2 é que ela não seja PI (ver Teorema de Kaplanski a seguir) ou pelo menos não localmente PI (toda subálgebra finitamente gerada é PI). Note que localmente PI não implica PI; ver [BRb] pág.10.

Como já citamos antes, a hipótese de dimensão infinita sobre o centro é de fato essencial. Para isso precisaremos de dois resultados. O primeiro deles é o famoso teorema de Wedderburn.

Teorema 2.2.3 ([GS06], pág.18)**.** *Seja D uma álgebra simples (os únicos ideais bilaterais são 0 e D) de dimensão finita sobre k. Então, existe um inteiro $n \geq 1$ e uma álgebra de divisão $D' \supset k$ tal que $D \approx M_n(D')$ (anel de matrizes). Além disso, D' é unicamente determinado a menos de isomorfismo.*

Corolário 2.2.4 ([GS06], pág.20)**.** *Seja k um corpo algebricamente fechado. Então, toda k-álgebra central simples A (k-álgebra simples cujo centro é k) é isomorfa a $M_n(k) $ para algum $n \geq 1$.*

Em nosso caso, o Teorema de Wedderburn só pode ser usado se $\dim_k D > 1$, enquanto o Corolário também vale quando a dimensão é 1, porém, faremos as duas análises. Se uma k-álgebra simples D é de dimensão finita sobre seu centro k, com $\dim_k D > 1$, pelo teorema de Wedderburn ela é isomorfa a um anel de matrizes $M_n(D')$ com $n > 1$ e coeficientes em uma álgebra de divisão D'. Como um anel de matrizes sobre um corpo é PI, não é possível encontrar k-álgebras livres em D, como foi analizado anteriormente. Quando $\dim_k D = 1$, precisamos necessariamente usar o Corolário anterior. Nesse caso, vale que

$$D \otimes_k \bar{k} \overset{\text{Cor. } 2.2.4}{\cong} M_m(\bar{k})$$

e então usamos que $D \hookrightarrow D \otimes_k \bar{k} \cong M_m(\bar{k})$ obtendo o mesmo resultado.

Temos também um resultado de Kaplansky (que vale mais geralmente, quando D é uma álgebra primitiva, ou seja, ele tem um módulo irredutível fiel (à direita ou à esquerda)) que é interessante citarmos:

Teorema 2.2.5 ([Kap48])**.** *Se D satisfaz qualquer identidade polinomial então D tem dimensão finita sobre k.*

Quando uma álgebra é infinitamente gerada sobre seu centro, ela pode não conter uma subálgebra livre, como mostra o seguinte

Exemplo 2.2.6. Considere o anel

$$\mathscr{M} = \bigcup_{n\geq 1} M_n(\overline{\mathbb{F}}_p),$$

de matrizes infinitas (apenas um número finito de entradas é não-nula) com entradas em $\overline{\mathbb{F}}_p$ (p primo). Qualquer conjunto finito de matrizes T em $\mathscr{M}$ está contido em algum anel de matrizes $M_r(\overline{\mathbb{F}}_p)$ para $r \gg 0$, ou seja, $\mathscr{M}$ não pode conter $\overline{\mathbb{F}}_p$-subálgebras livres de nenhum posto $n \geq 2$, pois caso contrário, o conjunto de geradores (conjunto finito) estaria contido em alguma extensão $M_r(\overline{\mathbb{F}}_p)$ de $\overline{\mathbb{F}}_p$ para $r \gg 0$, o que seria um absurdo.

A outra hipótese é com relação a D ser finitamente gerado sobre seu centro k. O exemplo anterior não é suficiente para mostrar que essa hipótese é importante. Neste caso temos o seguinte contra-exemplo:

Exemplo 2.2.7. Considere $k = \mathbb{F}_p((t))$, com p primo. Pela proposição 6.3.9 em [GS06] pág.150, temos que o grupo de Brauer $\mathrm{Br}(\mathbb{F}_p((t))) \cong \mathbb{Q}/\mathbb{Z}$. Considere um subconjunto $A \subset \mathbb{Q}/\mathbb{Z}$ infinito enumerável onde os índices dos elementos de A são dois a dois coprimos. Para cada elemento $a_n \in A$ obtemos uma álgebra cíclica D_{a_n} pela proposição 6.3.10 em [GS06] pág.151, no qual o índice (grau de $\widetilde{D}_{a_n}$ sobre k, onde $D_{a_n} = M_s(\widetilde{D}_{a_n})$ pelo Teorema de Wedderburn) é igual ao seu período (ordem de sua classe em $\mathrm{Br}(\mathbb{F}_p((t)))$). Desse modo, D_{a_n} é uma álgebra de divisão. Desde que os índices de D_{a_n} e D_{a_m} são coprimos, com $a_n \neq a_m$, segue que $D_{a_n} \otimes D_{a_m}$ é uma álgebra de divisão com centro $\mathbb{F}_p((t))$ ([FR93] pág.132 lema 4.18). Com isso, obtemos uma torre $D_{a_1} \subset D_{a_1} \otimes D_{a_2} \subset D_{a_1} \otimes D_{a_2} \otimes D_{a_3} \subset \cdots$, onde as inclusões são as óbvias. Note que cada uma dessas álgebras de divisão $D_{a_1} \otimes \ldots \otimes D_{a_n}$ ainda são finitamente geradas e de dimensão finita sobre $\mathbb{F}_p((t))$. Agora, considere D o limite direto dessas álgebras de divisão. Com isso, quaisquer dois elementos a, b em D estão contidos em alguma álgebra de divisão $D' = D_{a_1} \otimes \ldots \otimes D_{a_n}$, com n suficientemente grande, que é de dimensão finita sobre $\mathbb{F}_p((t))$. Pelo corolário acima, D' é injetado em um anel de matrizes por $D' \hookrightarrow D' \otimes_k \bar{k} \cong M_r(\bar{k})$. Pelo resultado de Amitsur e Levitzki citado acima, D' é PI e portanto a, b não geram uma álgebra livre em D sobre $\mathbb{F}_p((t))$.

2.3 Discussão e contra-exemplos II

Nessa seção, destacaremos quais hipóteses não podem ser enfraquecidas e quais não afetam a generalidade dos resultados ao longo deste trabalho. Seja L/k uma extensão de corpos com $L \neq k$ e σ um k-automorfismo de L.

Começamos com a hipótese de que k *é algebricamente fechado em* L. Essa não é uma hipótese restritiva, no sentido que se começamos com um corpo k que não é algebricamente fechado em L então podemos trocá-lo pela extensão intermediária $k' = L \cap \bar{k}$ que é algebricamente fechado em L. Isso não interfere nos resultados, pois pelo Lema 2.1.3 de Makar-Limanov e Malcolmson, não importa a escolha do corpo central (corpo base) quando procuramos por subálgebras livres.

Vamos impor que o corpo fixo por um automorfismo $\sigma : L \to L$ seja exatamente k. Isso inicialmente pode parecer restritivo, mas com relação a procura por subálgebras livres não há nenhum problema, novamente pelo Lema 2.1.3.

Supondo que $k = L^{\langle\sigma\rangle}$, então k algebricamente fechado em L implica que o k-automorfismo σ é de ordem infinita. De fato, se σ tem ordem finita n então todo elemento $f \in L \setminus k$ é raiz de

$$P(X) = \prod_{0 \leq i < n} (X - \sigma^i(f)),$$

que é um polinômio mônico de grau n com coeficientes em k (cada coeficiente é fixo por σ), ou seja, f é algébrico sobre k, o que é uma contradição, desde que k algebricamente fechado em L implica que todo elemento de $L \setminus k$ é transcendente sobre k.

Como consequência, variedades que possuem grupo de automorfismos finito não são interessantes para o nosso problema, pois em particular esses autormofismos têm ordem finita. Como exemplo, temos as curvas de gênero maior ou igual a 2: nesse caso, é conhecido que o seu grupo de automorfismos é finito por um famoso teorema de Hurwitz, de 1893, que diz que *uma curva não singular de gênero* g *pelo menos* 2, *tem no máximo* $84(g-1)$ *automorfismos*. Além disso, em [HMX] é provado que existe um limitante superior para o número de automorfismos birracionais de uma variedade de tipo geral, ou seja, uma variedade cuja dimensão projetiva do anel canônico é igual à dimensão da variedade (dimensão de Kodaira da variedade). Por exemplo, variedades abelianas têm dimensão de Kodaira zero e portanto não são de tipo geral.

Capítulo

3

Resultados gerais

Neste capítulo, descreveremos os resultados obtidos sobre o estudo da conjectura de Makar-Limanov quando consideramos o corpo skew $D = L(t;\sigma)$, onde L/k é uma extensão de corpos e σ é um k-automorfismo de L, com algumas hipóteses adicionais. Na primeira seção, apresentaremos algumas definições e notações . Na segunda seção, provaremos vários resultados que serão usados nas demonstrações do Lema 3.3.3 e do Teorema 3.3.5. Na terceira seção, provaremos que a conjectura de Makar-Limanov, sob certas hipóteses, é verdadeira para $D = L(t;\sigma)$. Com isso, na última seção, obteremos um caso particular da conjectura GA para D. Este capítulo compreende parte dos resultados que obtivemos inspirados pelos artigos [Lor86, GT12] e com isso, juntamente com o Capítulo Quatro, generalizamos esses dois trabalhos. Ao longo deste capítulo, o conjunto dos números naturais será $\mathbb{N} = \{0, 1, 2, \ldots\}$.

3.1 Setup

Definição 3.1.1. *Sejam k um corpo, L/k (com $L \neq k$) uma extensão de corpos tal que k é algebricamente fechado em L e σ um k-automorfismo de L. Escreva $\sigma_L \stackrel{def}{=} \mathrm{id} \otimes \sigma$ o automorfismo de $L \otimes_k L$ induzido por σ e escreva também σ_L para o automorfismo induzido em* $\mathrm{Frac}(L \otimes_k L)$ (*de agora em diante, estamos supondo que $L \otimes_k L$ é um domínio; essa discussão é bem detalhada na Seção* 1.3. *Como k é algebricamente fechado em L, $L \otimes_k L$ é um domínio se , por exemplo, k perfeito ou L/k separável*). *Assim:*

- *identifique* L *dentro de* $\mathrm{Frac}(L \otimes_k L)$ *pela aplicação* $L \hookrightarrow \mathrm{Frac}(L \otimes_k L)$ *tal que* $\ell \mapsto \ell \otimes 1$*;*

- $L_D \stackrel{def}{=} \{1 \otimes a \in L \otimes_k L; a \in L\}$*;*

- *seja* $\mathscr{F}$ *o anel das funções* $f : \mathbb{N} \to \mathrm{Frac}(L \otimes_k L)$ *quociente a relação de equivalência:* $f \sim g$ *se* $f(n) = g(n)$ *para todo* $n \gg 0$*. A soma e a multiplicação em* $\mathscr{F}$ *são feitas coordenada a coordenada. Note que* $\mathscr{F}$ *não é domínio pois, por exemplo, o elemento* $(0, 1, 0, 1, \ldots)$ *é divisor de zero em* $\mathscr{F}$*;*

- *defina o operador shift* $s : \mathscr{F} \to \mathscr{F}$ *por* $f^s(n) = f(n+1)$*, que é um automorfismo de* $\mathscr{F}$ *que restrito a* $\mathscr{C}$ *é a identidade;*

- *defina o operador* $\Delta : \mathscr{F} \to \mathscr{F}$ *por* $\Delta(f) = f^s - f$*; usando a mesma letra (de modo conveniente como veremos adiante) definimos* $\Delta : \mathrm{Frac}(L \otimes_k L) \to \mathrm{Frac}(L \otimes L)$ *por* $\Delta(f) = \sigma_L(f) - f$ *e também* $\Delta : L \to L$ *por* $\Delta(f) = \sigma(f) - f$*;*

- *seja* $f \in L \setminus k$ *e defina* $\gamma = \gamma_f \in \mathscr{F}$ *por* $\gamma(n) = (\mathrm{id} \otimes \sigma^n)(1 \otimes f) = \sigma_L^n(1 \otimes f)$ *para todo* $n \in \mathbb{N}$*;*

- *defina um morfismo de* k*-espaços vetoriais (não de anéis!)* $q : L[[t; \sigma]] \to \mathscr{F}$ *por* $\sum t^n a_n \mapsto (1 \otimes a_n)_{n \geq 0}$*.*

Observação 3.1.2.

- Para mudanças de base por L, aplicaremos sempre o funtor $L \otimes_k -$ (à esquerda), como na identificação de L em $\mathrm{Frac}(L \otimes_k L)$;

- identificamos $\mathrm{Frac}(L \otimes_k L)$ com $\mathscr{C} \subset \mathscr{F}$, onde $\mathscr{C}$ denotará o subconjunto das funções constantes de $\mathscr{F}$; elementos de $\mathscr{C}$ serão normalmente denotados por ϵ. Vale observar que esse não será o único modo de identificarmos $\mathrm{Frac}(L \otimes_k L)$ dentro de $\mathscr{F}$ e nem o que de fato queremos, como veremos na próxima seção;

- o morfismo q será usado para considerarmos os elementos de $L[[t; \sigma]]$ dentro de $\mathscr{F}$ e isso terá grande importância na demonstração do Teorema 3.3.5;

- note que tanto Δ quanto s podem ser definidos sem usar a relação de equivalência de $\mathscr{F}$;

- note que $\ker(q)$ é formado pelos polinômios em $L[[t; \sigma]]$;

- se $A \subset L$ é uma k-subálgebra de L tal que $\mathrm{Frac}(A) = L$, então o fato de $L \otimes_k L$ ser domínio, implica que $L \otimes_k A$ também é, e portanto, podemos considerar $\mathrm{Frac}(L \otimes_k A)$, que na verdade é igual a $\mathrm{Frac}(L \otimes_k L)$;

- k algebricamente fechado em L é equivalente a $L \cap \overline{k} = k$ e nesse caso, todo elemento de $L \setminus k$ é transcendente sobre k;

- em $L \otimes_k L$, se $1 \otimes a = 1 \otimes b$, com $a, b \in L$, então $a = b$. De fato, nesse caso $1 \otimes (a - b) = 0$, mas se $a - b \neq 0$ então podemos multiplicar a última expressão por $1 \otimes (a - b)^{-1}$, obtendo $1 \otimes 1 = 0$ o que é um absurdo pois $L \otimes_k L$ é domínio. Esse argumento será usado algumas vezes.

3.2 Lemas

Nessa seção, provaremos vários lemas. Começaremos com resultados sobre o anel $\mathscr{F}$.

O anel $\mathscr{F}$ foi definido para se tornar um anel auxiliar, de tal forma que contenha o corpo $\mathrm{Frac}(L \otimes_k L)$ e facilite as contas. Para isso, temos:

Lema 3.2.1. *Sejam L/k uma extensão de corpos tal que k é algebricamente fechado em L e σ um k-automorfismo de L.*

1. *A aplicação L-linear (da forma $\ell \otimes 1$)*

$$\begin{array}{rccc} \iota: & \mathrm{Frac}(L \otimes_k L) & \to & \mathscr{F} \\ & \xi & \mapsto & (\sigma_L^j(\xi))_{j \geq 0} \end{array} \tag{3.2.1}$$

   é um morfismo de anéis (e portanto injetor).

2. *O operador shift se restringe a $\iota(\mathrm{Frac}(L \otimes_k L))$ e também a $\iota(L \otimes_k L)$, e o diagrama abaixo é comutativo.*

$$\begin{array}{ccccc} L \otimes_k L & \hookrightarrow & \mathrm{Frac}(L \otimes_k L) & \xhookrightarrow{\iota} & \mathscr{F} \\ \downarrow{\scriptstyle \sigma_L} & & \downarrow{\scriptstyle \sigma_L} & & \downarrow{\scriptstyle s} \\ L \otimes_k L & \hookrightarrow & \mathrm{Frac}(L \otimes_k L) & \xhookrightarrow{\iota} & \mathscr{F} \end{array}$$

Demonstração: O item (1) é claro. O item (2) é direto: se $\xi \in \mathrm{Frac}(L \otimes_k L)$ e $\iota(\xi) = (\sigma_L^j(\xi))_{j \geq 0}$ então $s(\iota(\xi)) = (\sigma_L^{j+1}(\xi))_{j \geq 0} = \iota(\sigma_L(\xi))$.

■

Observação 3.2.2. Note que $q(f) = (1 \otimes f, 0, 0, \ldots) \notin \iota(\mathrm{Frac}(L \otimes L))$, para $f \in L^*$.

O próximo lema nos mostra o que acontece com elementos transcendentes de L sobre k após uma mudança de base.

Lema 3.2.3. *Sejam k um corpo, L/k uma extensão de corpos tal que k é algebricamente fechado em L, σ k-automorfismo de L e $f \in L \setminus k$ (logo transcendente sobre k). Então, $1 \otimes f$ é transcendente sobre L.*

Demonstração: Se $L[1 \otimes f] = L \otimes_k (k[f])$ então $\dim_L L[1 \otimes f] = \dim_L L \otimes_k (k[f]) = \dim_k k[f]$ e como f é transcendente sobre k, teríamos $1 \otimes f$ transcendente sobre L.

Note que um elemento de $L[1 \otimes f]$ é um somatório finito da forma

$$\sum_i (b_i \otimes 1)(1 \otimes f)^i = \sum_i b_i \otimes f^i,$$

onde $b_i \in L$, que claramente pertence a $L \otimes_k (k[f])$. Por outro lado, um elemento de $L \otimes_k (k[f])$ é um somatório finito da forma, onde $a_\ell \in L$ e $c_\ell^i \in k$,

$$\begin{aligned}
\sum_\ell \left(a_\ell \otimes (\sum_i c_\ell^i f^i) \right) &= \sum_\ell \left[\sum_i (a_\ell \otimes (c_\ell^i f^i)) \right] \\
&= \sum_i \left[\sum_\ell (a_\ell c_\ell^i \otimes 1)(1 \otimes f)^i \right] \\
&= \sum_i \left[\left(\sum_\ell a_\ell c_\ell^i \otimes 1 \right) (1 \otimes f)^i \right],
\end{aligned}$$

que é um elemento em $L[1 \otimes f]$. Isso encerra a demonstração.

■

Como foi dito anteriormente, a hipótese $k = L^{\langle\sigma\rangle}$ tem um papel importante neste trabalho. Porém, isso não será suficiente, precisaremos garantir que o mesmo acontece para qualquer potência do automorfismo.

Lema 3.2.4. *Sejam k um corpo, L uma extensão de k tal que k é algebricamente fechado em L e σ um k-automorfismo de L. Além disso, suponha que σ é tal que $k = L^{\langle\sigma\rangle}$. Então $k = L^{\langle\sigma^t\rangle}$, onde $L^{\langle\sigma^t\rangle}$ é o corpo fixo por σ^t e $t \in \mathbb{Z} \setminus \{0\}$.*

Demonstração: Primeiramente, note que se $\zeta \in L^{\langle\sigma^t\rangle}$, então

$$\prod_{0 \le i < |t|} (X - \sigma^i(\zeta))$$

é um polinômio mônico de grau $|t|$ anulado por ζ com coeficientes em k (basta aplicar σ em cada coeficiente e ver que eles serão fixos pelo automorfismo, portanto estão em k). Mas, ζ é um elemento qualquer de $L^{\langle\sigma^t\rangle}$, ou seja, a extensão $L^{\langle\sigma^t\rangle}/k$ é algébrica. Como k é algebricamente fechado em L, segue que $L^{\langle\sigma^t\rangle} = k$.

■

Lema 3.2.5. *Sejam k um corpo, L/k uma extensão de corpos tal que k é algebricamente fechado em L, σ um k-automorfismo de L tal que $k = L^{\langle\sigma\rangle}$ e $f \in L \setminus k$ (portanto, transcendente sobre k). Então, a função constante $\epsilon \stackrel{def}{=} \epsilon_f = 1 \otimes f \in \mathscr{C} \subset \mathscr{F}$ é transcendente sobre $\iota(\mathrm{Frac}(L \otimes L))$.*

Demonstração: Suponha que

$$\sum_j \xi_j (1 \otimes f)^j = 0,$$

onde $\xi_j \in \iota(\mathrm{Frac}(L \otimes L))$ não todos nulos, ou seja, $\xi_j = (\sigma_L^n(e_j))_{n\geq 0}$ e $e_j \in \mathrm{Frac}(L \otimes L)$ para cada j. Portanto,

$$\sum_j [\sigma_L^n(e_j)](1 \otimes f)^j = 0$$

para $n \gg 0$ (digamos $n > n_0$, para algum n_0). Com $n > n_0$ fixado estamos em $\mathrm{Frac}(L \otimes_k L)$, então, aplicando σ_L^{-n} obtemos

$$\sum_j e_j [\sigma_L^{-n}(1 \otimes f)^j] = \sum_j e_j [\sigma_L^{-n}(1 \otimes f)]^j = 0$$

para cada $n > n_0$. Com isso, se consideramos o polinômio não-nulo

$$g(X) = \sum_j e_j X^j \in (\mathrm{Frac}(L \otimes L))[X],$$

segue que g teria $\sigma_L^{-n}(1 \otimes f)$ como raiz para todo $n > n_0$. Mas, pelo Lema 3.2.4 temos que $1 \otimes f$ não é fixo por nenhuma potência do automorfismo σ_L. De fato, se existe $r > 0$ tal que $\sigma_L^r(1 \otimes f) = 1 \otimes f$, então $1 \otimes \sigma^r(f) = 1 \otimes f$ e pela Observação 3.1.2 obtemos $\sigma^r(f) - f = 0$, que é uma contradição pela escolha de f e pelo Lema 3.2.4. Portanto, os elementos $\sigma_L^{-n}(1 \otimes f)$ são todos distintos para $n > n_0$ e $g(X)$ tem infinitas raízes, que é um absurdo.

■

A próxima definição, assim como o próximo Lema, serão usados apenas no Lema 3.3.3.

Definição 3.2.6. *Para $J = (j_1, j_2, \ldots, j_{s+1}) \in \mathbb{N}_{>0}^{s+1}$ $(s > 0)$ ponha*

$$\beta_J(n) = \sum_{n > n_1 > \ldots > n_s > 0} \gamma(n_1)^{j_1} \gamma(n_2)^{j_2} \ldots \gamma(n_s)^{j_s} (1 \otimes f)^{j_{s+1}}$$

$(n \in \mathbb{N})$, onde γ foi definido na Seção 3.1. Para $s < 0$ ponha $J = \emptyset$, $\beta_\emptyset(n) = 1$ $\forall n > 0$ e $\beta_\emptyset(0) = 0$. Para $s = 0$, $\beta_J(n) = (1 \otimes f)^{j_1}$ para todo n, ou seja, $\beta_J = \epsilon^{j_1} \in \mathscr{C}$ é constante em $\mathscr{F}$.

Lema 3.2.7. *Sejam $\psi, \varphi : \mathbb{N} \to \mathrm{Frac}(L \otimes_k L)$. Então:*

1. $\Delta(\varphi\psi) = \varphi^s\Delta(\psi) + \Delta(\varphi)\psi$;
2. $\Delta(\beta_J) = \gamma^{j_1}\beta_{J(1)}$, *onde* $J = (j_1, ..., j_{s+1}) \in \mathbb{N}_{>0}^{s+1}$, $s > 0$ *e* $J(1) := (j_2, \ldots, j_{s+1})$. *Para* $s = 0$ *temos* $\Delta(\beta_J) = 0$ (*lembre que nesse caso* β_J *é constante*).

Demonstração:

1. Para $\psi, \varphi : \mathbb{N} \to \mathrm{Frac}(L \otimes_k L)$ temos:
$$\begin{aligned}\Delta(\varphi\psi) &= (\varphi\psi)^s - \varphi\psi \\ &= \varphi^s\psi^s - \varphi^s\psi + \varphi^s\psi - \varphi\psi \\ &= \varphi^s(\psi^s - \psi) + (\varphi^s - \varphi)\psi \\ &= \varphi^s\Delta(\psi) + \Delta(\varphi)\psi\end{aligned}$$
2. Aplicando Δ em β_J obtemos:
$$\begin{aligned}\Delta\beta_J(n) &= \beta_J(n+1) - \beta_J(n) \\ &= \sum_{n+1>n_1>\ldots>n_s>n_{s+1}=0} \gamma(n_1)^{j_1}\gamma(n_2)^{j_2}\ldots\gamma(n_s)^{j_s}(1\otimes f)^{j_{s+1}} \\ &- \sum_{n>n_1>\ldots>n_s>n_{s+1}=0} \gamma(n_1)^{j_1}\gamma(n_2)^{j_2}\ldots\gamma(n_s)^{j_s}(1\otimes f)^{j_{s+1}} \\ &= \sum_{n=n_1>n_2>\ldots>n_s>n_{s+1}=0} \gamma(n)^{j_1}\gamma(n_2)^{j_2}\ldots\gamma(n_s)^{j_s}(1\otimes f)^{j_{s+1}} \\ &= \gamma(n)^{j_1} \sum_{n>n_2>\ldots>n_s>n_{s+1}=0} \gamma(n_2)^{j_2}\ldots\gamma(n_s)^{j_s}(1\otimes f)^{j_{s+1}} \\ &= \gamma(n)^{j_1}\beta_{J(1)}(n)\end{aligned}$$

■

Uma hipótese sobre o automorfismo σ que usamos muito até agora é que $L^{\langle\sigma\rangle} = k$. Mas, o que ocorre após a mudança de base? Essa questão será respondida pelos próximos dois lemas.

Lema 3.2.8. *Sejam L/k uma extensão de corpos e σ um k-automorfismo de L tal que $L^{\langle\sigma\rangle} = k$. Seja A uma k-álgebra. Então, $(A \otimes_k L)^{\langle\sigma_A\rangle} = A$, onde $\sigma_A \overset{def}{=} \mathrm{id} \otimes \sigma$.*

Demonstração: Como $L^{\langle\sigma\rangle} = k$, então temos a seguinte sequência exata de k-módulos:

$$0 \longrightarrow k \longrightarrow L \overset{\sigma-id}{\longrightarrow} L.$$

Como A é uma k-álgebra, então ela é plana, e portanto

$$0 \longrightarrow A \longrightarrow A \otimes_k L \overset{\sigma_A-id}{\longrightarrow} A \otimes_k L$$

é exata e isso prova o lema.

■

Lema 3.2.9. *Sejam L/k uma extensão de corpos e σ um k-automorfismo de L tal que $L^{\langle\sigma\rangle} = k$. Seja A um k-domínio com $A \otimes_k L$ domínio . Então,* $(\mathrm{Frac}(A \otimes_k L))^{\langle\sigma_A\rangle} = \mathrm{Frac}(A)$*, onde induzimos σ_A no* $\mathrm{Frac}(A \otimes_k L)$ *usando a mesma notação.*

Demonstração: Seja $f \in (\mathrm{Frac}(A \otimes_k L))^{\langle\sigma_A\rangle}$. Defina o conjunto:

$$I_f \stackrel{def}{=} \{h \in A \otimes_k L; fh \in A \otimes_k L\}.$$

Claramente I_f é um ideal de $A \otimes_k L$. Além disso, $\sigma_A(I_f) \subset I_f$. De fato, se $h \in I_f$ então $f\sigma_A(h) = \sigma_A(fh) \in A \otimes_k L$, pois $\sigma_A(f) = f$.

Queremos provar que $f \in \mathrm{Frac}(A)$. Para isso, basta provar que $I_f \cap A \neq \{0\}$. De fato, se existe $h' \in A \setminus \{0\}$ tal que $fh' \in A \otimes_k L$, temos que $\sigma_A(fh') = fh'$ e portanto $fh' \in A$ pelo Lema 3.2.8, o que implica que $f \in \mathrm{Frac}(A)$ pois $h' \in A$.

Provaremos por contradição. Para isso, seja $h \in I_f \setminus L_D \cup A$ (casos triviais) e escreva

$$h = \sum_{i=1}^{n} a_i \otimes b_i.$$

Suponha que n é minimal (diremos que h é minimal) e portanto os a_i's são l.i. sobre k, assim como os b_i's. Considere o elemento $0 \neq h' \stackrel{def}{=} h \cdot (1 \otimes (1/b_1)) \in I_f$, que também é minimal com relação a n. Então, como $\sigma_A(I_f) \subset I_f$, $\Delta(h') \in I_f$ envolve um elemento a menos no somatório (pois $\Delta(a_1 \otimes 1) = 0$). Isso contradiz a minimalidade assumida, ou seja, $\sigma_A(h') = h'$. Pelo Lema 3.2.8, obtemos $\sigma_A(h') = h' \in A$, como queríamos.

■

3.3 O teorema

Nessa seção provaremos, sob certas hipóteses, que a conjectura de Makar-Limanov vale quando $D = \mathrm{Frac}(L[t;\sigma])$, onde L/k é uma extensão de corpos e σ é um k-automorfismo de L. Na verdade, provaremos um pouco mais, como veremos adiante. Mas, para obtermos esse resultado nesse grau de generalidade, estaremos sujeitos a uma condição que chamamos de *Hipótese do Delta*. Essa condição já apareceu em [Lor86], [GT09] (que na verdade vem dos primeiros resultados de Makar-Limanov) e mais recentemente em [BRb], dentre outros. Agora, vamos enunciar a *Hipótese do Delta* que será um dos passos importantes na demonstração do Lema 3.3.3. No capítulo quatro, mostraremos casos em que a *Hipótese do Delta* vale.

Hipótese do Delta 3.3.1. Sejam k um corpo, L/k uma extensão própria de corpos tal que k é algebricamente fechado em L e σ um k-automorfismo de L tal que $L^{\langle\sigma\rangle} = k$. Então

$$\Delta(L) \cap A \subset k,$$

para alguma k-subálgebra A de L com $\mathrm{Frac}(A) = L$

A partir de agora, escolhemos $f \in A \setminus k$ para alguma k-subálgebra A de L no qual vale a Hipótese do Delta. O lema a seguir será o principal ingrediente na prova do Teorema. Na verdade, é neste lema que usaremos a *Hipótese do Delta*.

Observação 3.3.2. Nos próximos resultados faremos alguns abusos de notação. Como a aplicação ι é injetora escreveremos $\iota(1 \otimes a) = 1 \otimes a$, com $a \in L$. Além disso, para elementos $b \in L_D$ escreveremos $b = 1 \otimes b$.

Lema 3.3.3. *Sejam k um corpo, L/k uma extensão própria de corpos tal que k é algebricamente fechado em L e σ um k-automorfismo de L tal que $L^{\langle\sigma\rangle} = k$. Suponha que vale a H. do Delta. Os elementos β_J são linearmente independentes sobre $\iota(L_D)$ em $\mathscr{F}$.*

Demonstração: Suponha que não vale o resultado. Para um multi-índice $J = (j_1, \cdots, j_s)$ escreva $|J| = s$ o tamanho dele e se $\mathscr{J}$ é um conjunto finito de índices J, ponha $|\mathscr{J}| = \max\{|J|; J \in \mathscr{J}\}$. Provaremos por indução em $|\mathscr{J}|$.

Seja $\sum_{J\in\mathscr{J}} e_J\beta_J = 0$ uma relação não trivial, onde $e_J \in \iota(L_D)^*$, escolhida da seguinte maneira:

(i) dentre todas as relações não triviais sobre $\iota(L_D)$, escolha aquela com $u = |\mathscr{J}| \geq 0$ minimal;

(ii) dentre as relações satisfazendo (i), escolha a relação em que o número de J's com $|J| = u$ é minimal.

Se $u \leq 1$, temos $\beta_{(j_1)} = (1 \otimes f)^{j_1}$ para $u = 1$ e $\beta_\emptyset = 1$ (constante) para $u = 0$. Note que os j's são distintos entre si. Pelo Lema 3.2.5, esses elementos são l.i. sobre $\iota(\mathrm{Frac}(L \otimes_k L))$ e portanto sobre $\iota(L_D)$, o que prova o primeiro passo de indução.

Para o caso geral ($u \geq 2$), reescreva a relação entre os β_J's da seguinte forma:

$$\sum_{|J|=u} e_J\beta_J = \sum_{|J|<u} d_J\beta_J \tag{3.3.2}$$

Podemos assumir que $e_J = 1$ para algum J tal que $|J| = u$ (todo e_J é invertível, assim, caso não existisse, poderíamos multiplicar por $1 \otimes (1/e_J)$, para algum J).

Para $J = (j_1, \ldots, j_s) \in \mathbb{N}^s$, segue do Lema 3.2.7 que

$$\Delta(e_J\beta_J) = \Delta(e_J) \cdot \beta_J + e_J^s\gamma^{j_1}\beta_{J(1)},$$

para $s \geq 2$ e $\Delta(e_J\beta_J) = \Delta(e_J) \cdot \beta_J$ se $s \leq 1$, onde $\Delta(e_J), e_J^s\gamma^{j_1} \in \iota(L_D)$ (pois L_D é estável por σ_L) e $|J(1)| < |J|$. Ou seja, aplicar Δ *não aumenta o número de J's com tamanho máximo.*

Aplicando Δ em ambos os lados de (3.3.2) obtemos

$$\sum_{|J|=u} \Delta(e_J) \cdot \beta_J + \sum_{|J|=u} e_J^s\gamma^{j_1}\beta_{J(1)} = \Delta\left(\sum_{|J|<u} d_J\beta_J\right) \tag{3.3.3}$$

Para o $e_J = 1$, temos que $\Delta(e_J) = 0$. Como $|J(1)| < |J|$, temos que o lado esquerdo de (3.3.3) tem pelo menos um termo a menos com $|J| = u$, enquanto no lado direito de (3.3.3) todos os termos têm tamanho $|J| < u$. Como os coeficientes em (3.3.3) ainda estão em $\iota(L_D)$, segue da minimalidade (ii) que todos eles são zero. Portanto, pela igualdade de termos com mesmo tamanho de J, obtemos:

(a) $\Delta(e_J) = 0$, para todo J tal que $|J| = u$;

(b) $\Delta(d_J) = \sum_{\substack{|I|=u \\ I(1)=J}} e_I^s\gamma^{i_1}$ para cada J fixado com $|J| = u-1$, onde $I = (i_1, \ldots, i_u)$.

Note que

$$\begin{aligned} 0 &= \Delta(e_J) \\ &\overset{\text{Obs } 3.3.2}{=} \Delta(\iota(1 \otimes e_J)) \\ &\overset{\text{Lema } 3.2.1}{=} \iota(\Delta(1 \otimes e_J)) \\ &= \iota(1 \otimes \Delta(e_J)), \end{aligned}$$

e assim, $1 \otimes \Delta(e_J) = 0$ pela injetividade de ι e portanto $\Delta(e_J) = 0$ ($e_J \in L$) pela Observação 3.1.2. Então, como $L^{\langle\sigma\rangle} = k$, (a) acontece se, e somente se, $e_J \in k^*$, para todo J com $|J| = u$. Para (b) temos:

$$\begin{aligned}
\iota(\Delta(d_J)) &\overset{\text{Lema } 3.2.1}{=} \Delta(\iota(d_J)) \\
&\overset{\text{Obs } 3.3.2}{=} \Delta(d_J) \\
&= \sum_{\substack{|I|=u \\ I(1)=J}} e_I^s \gamma^{i_1} \\
&\overset{e_I \in k}{=} \sum_{\substack{|I|=u \\ I(1)=J}} e_I \gamma^{i_1} \\
&\overset{def}{=} \sum_{\substack{|I|=u \\ I(1)=J}} e_I \iota(1 \otimes f)^{i_1} \\
&\overset{e_I \in k}{=} \sum_{\substack{|I|=u \\ I(1)=J}} (e_I \otimes 1)\iota(1 \otimes f)^{i_1} \\
&\overset{\text{Obs } 3.3.2}{=} \sum_{\substack{|I|=u \\ I(1)=J}} \iota(e_I \otimes 1)\iota(1 \otimes f)^{i_1} \\
&\overset{\text{Lema } 3.2.1}{=} \iota\Big(\sum_{\substack{|I|=u \\ I(1)=J}} e_I \otimes f^{i_1} \Big)
\end{aligned}$$

e assim, $\Delta(d_J) = \sum_{\substack{|I|=u \\ I(1)=J}} e_I \otimes f^{i_1}$ pela injetividade de ι. Portanto,

$$\Delta(d_J) \overset{\text{Obs } 3.3.2}{=} \Delta(1 \otimes d_J) = 1 \otimes \Delta(d_J) \overset{e_I \in k}{=} \sum_{\substack{|I|=u \\ I(1)=J}} 1 \otimes (e_I f^{i_1}). \tag{3.3.4}$$

Pela igualdade (3.3.4) e pela Observação 3.1.2, segue que

$$\Delta(d_J) = \sum_{\substack{|I|=u \\ I(1)=J}} e_I f^{i_1}, \tag{3.3.5}$$

com $d_J \in L$. Então, $\Delta(d_J) \in \Delta(L) \cap A \subset k$ pela *Hipótese do Delta* 3.3.1.

Para todo I, temos que cada $i_1 \geq 1$ (pois $i_1 \in \mathbb{N}_{>0}$) e que são distintos entre si. Mas f é transcendente sobre k, portanto, os e_I's na igualdade (3.3.5) são nulos. Como isso é feito para cada J com $|J| = u - 1$, obtemos $e_I = 0$ para todo I com $|I| = u$, o que é contradição pela minimalidade assumida em (i).

■

Agora, condicionado ao Lema 3.3.3, que por sua vez depende da *Hipótese do Delta* 3.3.1, vamos enunciar e provar o Teorema 3.3.5. A prova segue a linha de [Lor86] e [GT09].

Observação 3.3.4. No Teorema a seguir, quando L é finitamente gerado sobre k, estaremos nas hipóteses da Conjectura de Makar-Limanov: k é o centro de D (note que σ tem ordem infinita pelo Lema 3.2.4; como $L^{\langle\sigma\rangle} = k$, o resultado segue do Lema 1.1.14); claramente $\dim_k D$ é infinita; D é finitamente gerado como k-álgebra (por t e pelos geradores de L/k). Porém o resultado abaixo vale mesmo quando a extensão L não é finitamente gerada sobre k; obtemos assim um resultado mais geral.

Teorema 3.3.5. *Sejam k um corpo, L/k uma extensão própria de corpos tal que k é algebricamente fechado em L e σ um k-automorfismo de L tal que $L^{\langle\sigma\rangle} = k$. Seja $f \in A \setminus k$ para alguma k-subálgebra A de L no qual vale a Hipótese do Delta 3.3.1. Então, os elementos f e $t(1-t)^{-1}f$ geram uma álgebra livre sobre k em $D = L(t;\sigma)$.*

Demonstração: Primeiramente, lembre que definimos o morfismo de k-espaços vetoriais (não de anéis!) $q : L[[t;\sigma]] \to \mathscr{F}$ por $\sum t^n a_n \mapsto (1 \otimes a_n)_{n\geq 0}$. Vamos trabalhar inicialmente em $L((t;\sigma)) \supset D$, pois teremos $(1-t)^{-1} = 1+t+t^2+\cdots$. Depois, usando o morfismo q e a aplicação ι, faremos as contas em $\mathscr{F}$, o que facilitará nosso trabalho. Mostraremos que todos os monômios distintos em f e $t(1-t)^{-1}f$ são linearmente independentes sobre k. Esses monômios têm a forma

$$m_I = m_{(i_0,i_1,\cdots,i_v)} = f^{i_0}t(1-t)^{-1}f^{i_1}\cdots f^{i_{v-1}}t(1-t)^{-1}f^{i_v} \in L[[t;\sigma]],$$

onde v é o número de termos $t(1-t)^{-1}f$, $i_0 \geq 0$ e $i_1, \cdots, i_v \geq 1$.

Podemos escrever o monômio anterior como

$$\begin{aligned} m_I &= f^{i_0}\sum_{l_1\geq 1} t^{l_1}f^{i_1}\sum_{l_2\geq 1} t^{l_2}f^{i_2}\cdots\sum_{l_v\geq 1} t^{l_v}f^{i_v} \\ &= \sum_{l_1,\cdots,l_v\geq 1} t^{l_1+\cdots+l_v}(f^{i_0})^{\sigma^{l_1+\cdots+l_v}}(f^{i_1})^{\sigma^{l_2+\cdots+l_v}}\cdots(f^{i_{v-1}})^{\sigma^{l_v}}f^{i_v} \end{aligned}$$

Façamos a seguinte mudança de índices:

$$\begin{aligned} n &= l_1+\cdots+l_v \\ n_1 &= l_2+\cdots+l_v \\ &\vdots \\ n_{v-1} &= l_v \end{aligned}$$

no qual obteremos a seguinte expressão para os monômios:

$$\begin{aligned} m_I &= \sum_{n\geq 0} t^n \sum_{n>n_1>\cdots>n_{v-1}>0} f^{i_0\sigma^n+i_1\sigma^{n_1}+\cdots+i_{v-1}\sigma^{n_{v-1}}+i_v} \\ &= \sum_{n\geq 0} t^n \sum_{n>n_1>\cdots>n_{v-1}>0} f^{i_0\sigma^n} f^{i_1\sigma^{n_1}+\cdots+i_{v-1}\sigma^{n_{v-1}}+i_v} \\ &= \sum_{n\geq 0} t^n f^{i_0\sigma^n} \sum_{n>n_1>\cdots>n_{v-1}>0} f^{i_1\sigma^{n_1}+\cdots+i_{v-1}\sigma^{n_{v-1}}+i_v} \end{aligned}$$

para $v > 0$ e $m_I = f^{i_0}$ para $v = 0$.

Aplicando q em cada m_I obtemos $\overline{m_I} \overset{def}{=} q(m_I) = \gamma^{i_0}\beta_{I(1)}$ para $v > 0$ e $q(m_{(i_0)}) = (1 \otimes f^{i_0}, 0, 0, \ldots)$ para $v = 0$.

Considere então

$$\sum_I a_I m_I = \sum_{I\in\mathscr{I}_0} a_I m_I + \sum_{I\notin\mathscr{I}_0} a_I m_I = 0, \tag{3.3.6}$$

onde $a_I \in k$ e $\mathscr{I}_0 = \{(i_0, i_1, \cdots, i_v); v = 0\}$ (separamos os termos cujo vetor I tem tamanho 1). Aplicando q em (3.3.6) obtemos:

$$0 = \sum_I a_I \overline{m_I} = \sum_{I\in\mathscr{I}_0} a_I \overline{m_I} + \sum_{I\notin\mathscr{I}_0} a_I \overline{m_I}. \tag{3.3.7}$$

Como (3.3.7) é uma expressão em $\mathscr{F}$, o somatório sobre $I \in \mathscr{I}_0$ é zero pela relação de equivalência. Resta então

$$0 = \sum_{I\notin\mathscr{I}_0} a_I \overline{m_I} = \sum_{I\notin\mathscr{I}_0} (a_I\gamma^{i_0})\beta_{I(1)} = \sum_{J\neq\emptyset} \left(\sum_{I(1)=J} a_I\gamma^{i_0} \right) \beta_J,$$

onde $a_I\gamma^{i_0} \in \iota(L_D)$.

Pelo Lema 3.3.3, os β_J's são linearmente independentes sobre $\iota(L_D)$, portanto, para cada $J \neq \emptyset$, obtemos

$$0 = \sum_{I(1)=J} a_I\gamma^{i_0} \overset{\substack{\text{Obs}\\ 3.3.2;\\ a_I\in k}}{=} \iota\left(\sum_{I(1)=J} a_I \otimes f^{i_0} \right). \tag{3.3.8}$$

Assim,

$$\sum_{I(1)=J} a_I \otimes f^{i_0} = 0$$

pela injetividade de ι. Note que

$$\sum_{I(1)=J} a_I \otimes f^{i_0} \overset{a_I \in k}{=} 1 \otimes \left(\sum_{I(1)=J} a_I f^{i_0} \right) = 0.$$

Pela Observação 3.1.2

$$\sum_{I(1)=J} a_I f^{i_0} = 0.$$

Como os i_0's são distintos entre si (em particular no máximo um deles é zero), segue da transcendência de f sobre k que $a_I = 0$ para todo $I \notin \mathscr{I}_0$, pois a igualdade (3.3.8) vale para cada $J \neq \emptyset$. A expressão (3.3.6) se reduz a

$$\sum_{I \in \mathscr{I}_0} a_I m_I \overset{def}{=} \sum_{I=(i_0) \in \mathscr{I}_0} a_I f^{i_0} = 0.$$

Usando novamente que f é transcendente sobre k e que os i_0's são distintos entre si, obtemos $a_I = 0$ para todo $I \in \mathscr{I}_0$. Isso encerra a prova.

■

3.4 Conjectura GA

Nesta seção, veremos como obter um caso particular da conjectura GA, generalizando [GT12]. Para isso, utilizaremos o Teorema 3.3.5 e o seguinte teorema de Lichtman, já citado no Capítulo Dois:

Teorema 3.4.1. *Seja $D = \operatorname{Frac} R$ com centro k, onde R é um domínio de Ore com uma valorização discreta v. Suponha que elementos a, b geram uma k-subálgebra livre em D. Se $v(a) \geq 1$ e $v(b) \geq 1$, então os elementos $1 + a, 1 + b$ geram o anel de grupo do grupo livre de posto 2 em D.*

Provaremos o seguinte:

Nas hipóteses do Teorema 3.3.5, suponha que os elementos f e $t(1-t)^{-1}f$ geram uma álgebra livre sobre k em $D = L(t; \sigma)$. Então, a conjectura GA vale para $D = L(t; \sigma)$.

Antes da demonstração, vejamos a definição de valorização no caso não-comutativo.

Definição 3.4.2. *Seja D um anel de divisão, $(G, *, <)$ um grupo totalmente ordenado e $\infty \notin G$ satisfazendo $g * \infty = \infty * g = \infty$, para todo $g \in G$. Uma aplicação*

$$v : D \mapsto G \cup \{\infty\}$$

é uma valorização sobre D se:

(i) $v(0) = \infty$*;*

(ii) $v(ab) = v(a) * v(b)$*, para todo* $a, b \in D$*;*

(iii) $v(a + b) \geq \min\{v(a), v(b)\}$*, para todo* $a, b \in D$*.*

Demonstração: Como os elementos f e $g = t(1 - t)^{-1}f$ geram uma k-subálgebra livre em $D = L(t; \sigma)$, os elementos fg e g também geram uma k-subálgebra livre em D.

Considere em $L((t; \sigma))$ a valorização $v : L((t; \sigma)) \mapsto \mathbb{Z} \cup \{\infty\}$ com a seguinte propriedade: v é trivial sobre L e $v(t) = 1$. Como $v(f) = 0$, temos que $v(fg) = v(g)$. Note que $v((1 - t)^{-1}) = 0$, pois $(1 - t)^{-1}$ é inversível em $L((t; \sigma))$[1]. Portanto,

$$v(fg) = v(g) = v(t) + v((1 - t)^{-1}) + v(f) = v(t) = 1.$$

Pelo Teorema 3.4.1, os elementos $1 + fg$ e $1 + g$ geram uma álgebra de grupo do grupo livre de posto 2 em D sobre k.

■

[1] se $ab = 1$, então $v(a) + v(b) = 0$.

Capítulo

4

Hipótese do Delta

Já provamos o Teorema 3.3.5 assumindo a *Hipótese do Delta*. Neste capítulo verificaremos casos em que essa condição vale, que são alguns dos principais resultados que obtivemos. Mas antes, vamos provar um Lema.

Lema 4.0.3. *Sejam k um corpo e X um esquema noetheriano integral separado regular sobre k com corpo de funções F. Seja Σ um automorfismo de X e σ automorfismo de F induzido por Σ. Seja $\Delta : F \to F$ definido por $g \mapsto \sigma(g) - g$, com $g \in F$. Então, se $\Delta(g)$ tem no máximo um polo (sem contar multiplicidade), segue que g e $\sigma(g)$ têm o mesmo conjunto de polos sem multiplicidade.*

Demonstração: Seja $g \in F$ um elemento não nulo e seja $S \subset X$ o conjunto dos polos de g sem multiplicidade (que é finito! Ver [Har77] pág.131).

Temos que $T = \Sigma^{\sharp} S = \{\Sigma^{-1} D; D \in S\}$ é o conjunto dos polos de $\sigma(g)$. Portanto, $|S| = |T|$. É fato que o conjunto de polos de $\Delta(g)$ contém os polos de g e $\sigma(g)$, exceto possivelmente os elementos de $S \cap T$, ou seja, contém $S \cup T \setminus S \cap T$. Esse conjunto tem cardinalidade $2(|S| - |S \cap T|)$ (direto do fato de $|S| = |T|$).

Suponha que $\Delta(g)$ tem no máximo um polo (sem contar multiplicidade). Como o conjunto de polos dos $\Delta(g)$ contém a diferença simétrica, obtemos $|S \cup T \setminus S \cap T| \leq 1$. Mas já sabemos que $|S \cup T \setminus S \cap T| = 2(|S| - |S \cap T|)$ e portanto, $|S \cup T \setminus S \cap T| = 0$, ou seja, $S = T$.

■

4.1 Variedades Abelianas

Nessa seção verificaremos que a *Hipótese do Delta* é verdadeira quando o automorfismo σ é induzido por um automorfismo de uma variedade abeliana. Suponha que:

- $k = \mathbb{C}$ (essa escolha do corpo é feita somente para usarmos o Teorema de Kronecker 1.2.13; $k = \bar{k}$ é a exigência mínima do Teorema de Bertini 1.2.11);
- X é uma variedade abeliana sobre $\mathbb{C}$ de $\dim_{\mathbb{C}} X \geq 2$. Como foi dito no Capítulo 1, uma variedade abeliana é necessariamente projetiva e isso nos permitirá usar o Teorema de Bertini; escreva $L = \mathcal{O}_{X,\xi}$, onde ξ é o ponto genérico de X;
- H é um hiperplano genérico, dado pelo Teorema de Bertini (como $\dim_{\mathbb{C}} X \geq 2$, ainda pelo Teorema de Bertini temos que $X \setminus X \cap H$ é irredutível); o caso de dimensão 1 pode ser resolvido de outra maneira: ver [GT09];
- $f \in \mathcal{O}_X(X \setminus H) \setminus \mathbb{C}$. Note que de fato existem seções não constantes, pois H é hiperplano com $X \setminus H$ irredutível ($\dim_{\mathbb{C}} X \geq 2$), portanto $X \setminus H$ é aberto afim;
- Σ é a translação por um ponto $P_0 \in X$ tal que $\{nP_0\}$ é denso em X para todo $n \in \mathbb{N}$ (a maioria dos vetores satisfaz essa condição; ver Teorema de Kronecker). Além disso, se $Q \in X$ então $Q + nP_0$ também é denso em X (direto do Teorema de Kronecker).
- Nesse caso, o automorfismo induzido σ satisfaz $L^{\langle\sigma\rangle} = \mathbb{C}$, por causa da órbita densa de P_0.

Lema 4.1.1 (*Hipótese do Delta*)**.** *Nas hipóteses acima temos que*

$$\Delta(L) \cap \mathcal{O}_X(X \setminus H) \subset \mathbb{C}.$$

Demonstração: Sejam $g \in L$ e $S \subset X$ o conjunto dos polos de g sem multiplicidade. Seja também T o conjunto de polos de $\sigma(g)$. Suponha que $\Delta(g) \in \mathcal{O}_X(X \setminus H)$. Qualquer elemento de $\mathcal{O}_X(X \setminus H)$ tem no máximo um polo em H, ou seja, pelo Lema 4.0.3 segue que $S = T$. Porém, se $S \neq \emptyset$, como $S = T = \Sigma^\sharp S \overset{def}{=} \{D - P_0; D \in S\}$ temos que o conjunto dos polos de g seria estabilizado por Σ e assim alguma potência de Σ fixaria cada elemento de S. Isso nos diz que a órbita de pontos na união (finita) desses hiperplanos ainda estaria contida nessa união, mas isso é impossível pois a órbita de P_0 é densa e consequentemente, órbitas de pontos nessa união também são densas em

X. Portanto, $S = \emptyset$. Como X é projetivo, uma função sem polos é constante, ou seja, $\Delta(g) \in \mathbb{C}$.

■

4.2 Espaço Projetivo

Aqui provaremos que a *Hipótese do Delta* é verdadeira quando consideramos o espaço projetivo n-dimensional.

Seja k um corpo. Sejam V um espaço vetorial de dimensão finita $n+1$ sobre k, $X = \mathbb{P}(V)$ o espaço projetivo n-dimensional e Σ um k-automorfismo de $\mathbb{P}(V)$ de ordem infinita tal que k seja exatamente o corpo fixo pelo automorfismo σ induzido por Σ em $L = \mathrm{PGL}_n(k)$.

FATO GERAL: se um elemento de $\mathrm{PGL}(V)$ fixa $n+2$ pontos de $\mathbb{P}(V)$ então ele é a identidade. Note que o mesmo vale para $\mathbb{P}(V^*)$.

Lema 4.2.1. *Nessas condições, existe um hiperplano H de $\mathbb{P}(V)$ tal que $\Sigma^i H \neq H$ para todo $i > 0$.*

Demonstração: Temos uma bijeção

$$\begin{array}{rccc} \Gamma: & \mathrm{Hip}(\mathbb{P}(V)) & \to & \mathbb{P}(V^*) \\ & H = \{h = 0\} & \mapsto & [h] \end{array}$$

entre o conjunto dos hiperplanos de $\mathbb{P}(V)$ e os pontos de $\mathbb{P}(V^*)$, onde $h \in V^*$ e $[h]$ é a classe de h em $\mathbb{P}(V^*)$. Além disso, Σ induz um automorfismo

$$\begin{array}{rccc} \Sigma': & \mathrm{Hip}(\mathbb{P}(V)) & \to & \mathrm{Hip}(\mathbb{P}(V)) \\ & H = \{h = 0\} & \mapsto & \{\Sigma^\sharp(h) = h \circ \Sigma^{-1} = 0\} \end{array}$$

Note que $h \circ \Sigma^{-1}(p) = 0 \Leftrightarrow \Sigma^{-1}(p) \in H \Leftrightarrow p \in \Sigma(H)$. Desse modo, temos um automorfismo $\Sigma'' : \mathbb{P}(V^*) \to \mathbb{P}(V^*)$, dado por $[h] \mapsto [h \circ \Sigma^{-1}]$. Portanto, obtemos o seguinte diagrama comutativo:

$$\begin{array}{ccc} \mathrm{Hip}(\mathbb{P}(V)) & \xhookrightarrow[\Gamma]{} & \mathbb{P}(V^*) \\ {\scriptstyle \Sigma'}\downarrow & & \downarrow{\scriptstyle \Sigma''} \\ \mathrm{Hip}(\mathbb{P}(V)) & \xhookrightarrow[\Gamma]{} & \mathbb{P}(V^*) \end{array}$$

Isso nos dá uma correspondência bijetora entre automorfismos de $\mathrm{Hip}(\mathbb{P}(V))$ e automorfismos de $\mathbb{P}(V^*)$.

Considere $M = \{H; H \text{ é hiperplano tal que } \Sigma^i H = H \text{ para algum } i > 0\}$. Sejam $H_i = \{h_i = 0\}$ com $i = 1, \ldots, n+2$, hiperplanos distintos em M fixados por potências α_i

de Σ respectivamente, com $i = 1, \ldots, n+2$. Temos que $(\Sigma')^{\alpha_i}(H_i) = H_i$. Pelo diagrama comutativo, esses hiperplanos correspondem a pontos distintos P_i em $\mathbb{P}(V^*)$, respectivamente, que são fixos pelas respectivas potências de Σ''. Então, $(\Sigma'')^{\alpha_1\alpha_2\ldots\alpha_{n+2}} = (\Sigma'')^{\alpha}$ fixa $n+2$ pontos e pelo *fato geral* segue que $(\Sigma'')^{\alpha} = \mathrm{id}$ implicando que $(\Sigma')^{\alpha} = \mathrm{id}$. Portanto, Σ^{α} fixa todo hiperplano de $\mathbb{P}(V)$. Sabemos que todo ponto $x \in \mathbb{P}(V)$ pode ser visto como a interseção de n hiperplanos e portanto, $\Sigma^{\alpha}(x) = x$ para todo $x \in \mathbb{P}(V)$. Desse modo, $\Sigma^{\alpha} = \mathrm{id}$, o que seria um absurdo. Portanto, $|M| \leq n+1$. Por contagem de elementos de $\mathbb{P}(V^*)$, existe um ponto P que não é fixo por nenhuma potência de Σ'', que corresponde a um hiperplano H de $\mathbb{P}(V)$ que não é fixo por nenhuma potência de Σ, como queríamos.

■

Lema 4.2.2 (*Hipótese do Delta*)**.** *Sejam $X = \mathbb{P}(V)$ o espaço projetivo n-dimensional, Σ um k-automorfismo de $\mathbb{P}(V)$ de ordem infinita tal que o automorfismo induzido σ em L satisfaz $L^{\langle\sigma\rangle} = k$ e H o hiperplano dado pelo Lema 4.2.1. Então:*

$$\Delta(L) \cap \mathcal{O}_X(X \setminus H) \subset k.$$

Demonstração: Sejam $g \in L$ e $S \subset X$ o conjunto dos polos de g sem multiplicidade. Seja também T o conjunto de polos de $\sigma(g)$.

Suponha que $\Delta(g) \in \mathcal{O}_X(X \setminus H)$. Qualquer elemento de $\mathcal{O}_X(X \setminus H)$ tem no máximo um polo em H. Pelo Lema 4.0.3 temos $S = T = \Sigma^{\sharp}S$. Porém, se $S \neq \emptyset$, então o conjunto de polos de g é estabilizado por Σ e portanto, alguma potência de Σ fixa todos os pontos de S. Por hipótese $H \notin S = T$ e então H não é polo de $\Delta(g)$ que portanto deve ser constante.

■

Referências Bibliográficas

[AL50] A. S. Amitsur and J. Levitzki. Minimal identities for algebras. *Proc. Amer. Math. Soc.*, 1:449–463, 1950.

[BL04] C. Birkenhake and H. Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BRa] J. P. Bell and D. Rogalski. Free subalgebras of division algebras over uncountable fields. *arXiv:1112.0041*.

[BRb] J. P. Bell and D. Rogalski. Free subalgebras of quotient rings of ore extensions. *arXiv:1101.5829*.

[Car] P. Cartier. *Séminaire Henri Cartan de l'Ecole Normale Supérieure, 1955/1956. Extensions régulières*. tome 8, exp.14, p. 1-10.

[Coh77] P. M. Cohn. *Skew field constructions*. Cambridge University Press, Cambridge, 1977. London Mathematical Society Lecture Note Series, No. 27.

[Coh06] P. M. Cohn. *Free ideal rings and localization in general rings*, volume 3 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[CS86] G. Cornell and J. H. Silverman, editors. *Arithmetic geometry*. Springer-Verlag, New York, 1986. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984.

[Deb05] O. Debarre. *Complex tori and abelian varieties*, volume 11 of *SMF/AMS Texts and Monographs*. American Mathematical Society, Providence, RI, 2005. Translated from the 1999 French edition by Philippe Mazaud.

[FGS96] L. M. V. Figueiredo, J. Z. Gonçalves, and M. Shirvani. Free group algebras in certain division rings. *J. Algebra*, 185(2):298–313, 1996.

[FR93] B. Farb and Dennis R.K. *Noncommutative algebra*, volume 144 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993.

[GS06] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[GT09] J. Z. Gonçalves and E. Tengan. A note on free groups in the ring of fractions of skew polynomial rings. *Comm. Algebra*, 37(7):2477–2484, 2009.

[GT12] J. Z. Gonçalves and E. Tengan. Free group algebras in division rings. *Internat. J. Algebra Comput.*, 22(5), 2012.

[GW89] K. R. Goodearl and R. B. Warfield, Jr. *An introduction to noncommutative Noetherian rings*, volume 16 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1989.

[Har77] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[HMX] C.D. Hacon, J Mckernan, and C. XU. On the birational automorphism of varieties of general type. *arXiv:1011.1464*.

[Kap48] I. Kaplansky. Rings with a polynomial identity. *Bull. Amer. Math. Soc.*, 54:575–580, 1948.

[Lam01] T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[Lan83] S. Lang. *Abelian varieties*. Springer-Verlag, New York, 1983. Reprint of the 1959 original.

[Lan02] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Lic77] A. I. Lichtman. On subgroups of the multiplicative group of skew fields. *Proc. Amer. Math. Soc.*, 63(1):15–16, 1977.

[Lic78] A. I. Lichtman. Free subgroups of normal subgroups of the multiplicative group of skew fields. *Proc. Amer. Math. Soc.*, 71(2):174–178, 1978.

[Lic82] A. I. Lichtman. On normal subgroups of multiplicative group of skew fields generated by a polycyclic-by-finite group. *J. Algebra*, 78(2):548–577, 1982.

[Lic84] A. I. Lichtman. On matrix rings and linear groups over fields of fractions of group rings and enveloping algebras. II. *J. Algebra*, 90(2):516–527, 1984.

[Liu02] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[Lor86] M. Lorenz. On free subalgebras of certain division algebras. *Proc. Amer. Math. Soc.*, 98(3):401–405, 1986.

[Mat80] H. Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[Mat89] H. Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[Mila] J.S. Milne. Abelian varieties. *http://www.jmilne.org/math/CourseNotes/AV.pdf*.

[Milb] J.S. Milne. Algebraic geometry. *http://www.jmilne.org/math/CourseNotes/AG.pdf*.

[ML83] L. Makar-Limanov. The skew field of fractions of the Weyl algebra contains a free noncommutative subalgebra. *Comm. Algebra*, 11(17):2003–2006, 1983.

[ML84a] L. Makar-Limanov. On free subobjects of skew fields. In *Methods in ring theory (Antwerp, 1983)*, volume 129 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 281–285. Reidel, Dordrecht, 1984.

[ML84b] L. Makar-Limanov. On group rings of nilpotent groups. *Israel J. Math.*, 48(2-3):244–248, 1984.

[ML91] L. Makar-Limanov. On subalgebras of the first Weyl skewfield. *Comm. Algebra*, 19(7):1971–1982, 1991.

[MLM91] L. Makar-Limanov and P. Malcolmson. Free subalgebras of enveloping fields. *Proc. Amer. Math. Soc.*, 111(2):315–322, 1991.

[MMST11] F. B. Martinez, C. G. Moreira, N. Saldanha, and E. Tengan. *Teoria dos números*. Projeto Euclides. Second edition, 2011.

[Mum08] D. Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[Rei96] Z. Reichstein. On a question of Makar-Limanov. *Proc. Amer. Math. Soc.*, 124(1):17–19, 1996.

[Sán] J. Sánchez. Free group algebras in Malcev-Neumann skew field of fractions. *arXiv:1107.2429*.

[SG96] M. Shirvani and J. Z. Gonçalves. On free group algebras in division rings with uncountable center. *Proc. Amer. Math. Soc.*, 124(3):685–687, 1996.

[SG98] M. Shirvani and J. Z. Gonçalves. Free group algebras in the field of fractions of differential polynomial rings and enveloping algebras. *J. Algebra*, 204(2):372–385, 1998.

[SG99] M. Shirvani and J. Z. Gonçalves. Large free algebras in the ring of fractions of skew polynomial rings. *Journal of the London Mathematical Society (2)*, 60(2):481–489, 1999.

[SG12] M. Shirvani and J. Z. Gonçalves. A survey on free objects in division rings and in division rings with an involution. *Comm. Algebra*, 40(5):1704–1723, 2012.

[Smo09] A. Smoktunowicz. Makar-Limanov's conjecture on free subalgebras. *Adv. Math.*, 222(6):2107–2116, 2009.

[Sta] Stacks project. *http://stacks.math.columbia.edu*.

[Tit72] J. Tits. Free subgroups in linear groups. *J. Algebra*, 20:250–270, 1972.