UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Uma conjectura de Artin e sua resolução por Ax e Kochen via Teoria de Modelos

por

Samuel Volkweis Leite

Dissertação submetida como requisito parcial
para a obtenção do grau de
Mestre em Matemática

Profa. Dra. Cydara Cavedon Ripoll
Orientadora

Porto Alegre, junho de 2009

Uma conjectura de Artin e sua resolução por Ax e Kochen via Teoria de Modelos

por

Samuel Volkweis Leite[1]

Dissertação submetida ao Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de

Mestre em Matemática

Linha de Pesquisa: Álgebra

Orientadora: Profa. Dra. Cydara Cavedon Ripoll

Banca examinadora:

Prof. Dr. Antonio José Engler
IMECC/UNICAMP-SP

Profa. Dra. Ada Maria de Souza Doering
IM/UFRGS-RS

Profa. Dra. Luisa Rodriguez Doering
IM/UFRGS-RS

Dissertação apresentada
18 de Junho de 2009.

Prof. Dr. Jaime Bruck Ripoll
Coordenador

[1]Bolsista do CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico

AGRADECIMENTOS

Agradeço aos meus pais pela educação e amor que me deram, ao meu irmão por ser meu maior incentivador e motivador para o início de meus estudos em matemática, aos meus colegas por todos os momentos felizes e de aprendizado que passamos juntos, ao meu Amor por ter aparecido no momento certo na minha vida e por ter me feito uma pessoa muito mais completa e feliz.

Também agradeço à dedicação, apoio e compreensão que recebi de minha orientadora, Profa. Dra. Cydara Cavedon Ripoll, em todos os momentos em que trabalhamos juntos. Me sinto muito grato pela oportunidade de conviver com uma pessoa que é um exemplo a ser seguido como profissional e ser humano. Finalmente, agradeço ao Prof. Dr. Alexander Prestel pela sugestão do assunto dessa dissertação e pelo trabalho desenvolvido em prol da matemática, pois graças aos livros de sua autoria, sendo um escrito em co-autoria com o Prof. Dr. Antonio José Engler, consegui escrever o presente trabalho.

Agradeço ao CNPq pelo apoio financeiro e ao PPGMAT da UFRGS pela oportunidade de aprendizado que recebi.

Existe um paralelismo fiel entre o progresso social e a atividade matemática, os países socialmente atrasados são aqueles em que a atividade matemática é nula ou quase nula.

Jacques Chapellon

A Matemática é a honra do espírito humano.

Leibniz

O grande arquiteto do Universo começa a parecer-nos um puro matemático.

James Jeans

RESUMO

O presente trabalho tem por objetivo apresentar a prova de um teorema de James Ax e Simon B. Kochen relacionada com uma conjectura de Artin. A demontração apresentada usa essencialmente Teoria de Modelos e Teoria de Valorizações.

O teorema nos diz que para cada grau $d \in \mathbb{N}^*$ existe uma cota n_d tal que, para todo primo $p \geq n_d$, cada polinômio homogêneo sobre $\mathbb{Q}_p$ de grau d em mais de d^2 variáveis possui uma raiz não trivial no corpo de números p-ádicos $\mathbb{Q}_p$.

A solução encontrada por Ax e Kochen para a conjectura de Artin é um dos mais importantes exemplos de aplicação de Teoria de Modelos — um ramo da Lógica Matemática — à Álgebra, neste caso, à Teoria de Números.

ABSTRACT

The present work has objective to present a proof of a theorem due to James Ax and Simon B. Kochen related to an Artin's conjecture. The demonstration shown uses essencially Model Theory and Valuation Theory.

The theorem tell us that for each degree $d \in \mathbb{N}^*$ exists a bound n_d such that, for all prime $p \geq n_d$, each homogeneous polynomial over $\mathbb{Q}_p$ of degree d in more than d^2 variables has a non-trivial root in the field of p-adic numbers $\mathbb{Q}_p$.

The solution found by Ax and Kochen for the Artin's conjecture is one of the most important examples of application of Model Theory — a branche of Mathematical Logic — to Algebra, in this case, to Number Theory.

Sumário

1 Notações

Em geral:

$P(S)$ o conjunto das partes de um conjunto S

$\mathbb{P}$ o conjunto dos números primos

K um corpo (não necessariamente de característica zero)

$A^{\times}$ = invertíveis do anel A

$\mathbb{R}_{+}$ = reais não-negativos

Para a Teoria de Valorizações:

$|\ |$ = valor absoluto em um corpo K

$|\ |_0$ = valor absoluto usual de $\mathbb{R}$

$Res(f, g)$ = a resultante entre os polinômios f e g

$\widetilde{K}$ = um fecho algébrico de K

$K^s = \{\alpha \in \widetilde{K} \mid \alpha$ é separável sobre $K\}$

Para a Teoria de Modelos

$\mathcal{L}$ = uma linguagem formal de primeira ordem

$\mathcal{L}'$ = extensão da linguagem $\mathcal{L}$

Símbolos lógicos : $\neg$ (negação) , $\wedge$ (e), $\forall$ (para todo), $\doteq$ (igual), $\vee$ (ou), $\exists$ (existe).

Variáveis : $v_0, ..., v_n, ...$ $(n \in \mathbb{N})$

Símbolos relacionais : R_i $(i \in I)$

Símbolos funcionais : f_j $(j \in J)$

Símbolos constantes : c_k $(k \in K)$

Vbl = o conjunto de todas as variáveis.

$Sent_{\mathcal{L}}$ = conjunto das sentenças em uma linguagem $\mathcal{L}$

$For_{\mathcal{L}}$ = conjunto das fórmulas em uma linguagem $\mathcal{L}$

$Tm_{\mathcal{L}}$ = conjunto dos termos em uma linguagem $\mathcal{L}$

$\mathcal{L} = (\lambda, \mu, K)$ a assinatura da linguagem $\mathcal{L}$ (identificamos a linguagem com a sua assinatura)

$Fr(\psi)$ = conjunto das variáveis livres de ψ

$\zeta(v/t)$ = fórmula obtida da fórmula ζ pela substituição de cada ocorrência livre da variável v pelo termo t

$\zeta(x_1/t_1, ..., x_n/t_n)$ = fórmula obtida da fórmula ζ pela substituição de cada ocorrência livre de x_i pelo termo t_i, para cada $i \in \{1, ..., n\}$

$\vdash \varphi$: leia-se "φ é dedutível"

$\Sigma \vdash \varphi$: leia-se "dedutível de Σ"

$(\varphi_1, ..., \varphi_n)$ com $\varphi_i \in Fml_{\mathcal{L}}$ representa uma prova na linguagem $\mathcal{L}$

TC = conjunto dos termos constantes

$TC/\approx$ = modelo de termos

$\mathfrak{A}$ = uma $\mathcal{L}$-estrutura

$|\mathfrak{A}|$ = domínio da $\mathcal{L}$-estrutura $\mathfrak{A}$

$\mathcal{L}_{\mathfrak{A}}$ ou $\mathcal{L}(\mathfrak{A})$ = linguagem ampliada de $\mathcal{L}$ por constantes a partir do domínio da $\mathcal{L}-$estrutura $\mathfrak{A}$.

$t^{\mathfrak{A}}[h]$ = valor do termo t pela avaliação h em $\mathfrak{A}$

$\mathfrak{A} \models \varphi[h]$: leia-se "em $\mathfrak{A}$ vale φ por h"

$\mathfrak{A} \not\models \varphi[h]$: leia-se "em $\mathfrak{A}$ não vale φ por h"

$\mathfrak{A} \models \varphi$: leia-se "em $\mathfrak{A}$ vale φ por qualquer h"

$\mathfrak{A} \models \forall\varphi$: entenda-se ($\forall\varphi$ está no lugar de $\forall x_1, ..., x_n\ \varphi$, com $Fr(\varphi) \subset \{x_1, ..., x_n\}$.)

$\mathfrak{A} \models \Sigma$ significa que $\mathfrak{A}$ é um modelo para o conjunto de sentenças Σ

$Th_{\mathcal{L}}(M) = \mathcal{L}-$teoria de M, um conjunto não vazio de $\mathcal{L}-$estruturas

T ou $Th_{\mathcal{L}}(\mathfrak{A})$ ou $Th(\mathfrak{A})$ = teoria da $\mathcal{L}-$estrutura $\mathfrak{A}$ (ou do conjunto $\{\mathfrak{A}\}$)

M_T = a classe dos modelos de T, onde T é uma teoria, em particular um conjunto de sentenças.

$Mod_{\mathcal{L}}$ a classe de todas as $\mathcal{L}$-estruturas

$Mod_{\mathcal{L}}(\Sigma)$ = a classe dos modelos de Σ

$Ded_{\mathcal{L}}(\Sigma)$ = conjunto das $\mathcal{L}$-sentenças que podem ser deduzidas de Σ

$\mathfrak{A} \equiv \mathfrak{A}'$: leia-se "$\mathfrak{A}$ e $\mathfrak{A}'$ são elementarmente equivalentes

$\tau : \mathfrak{A} \leftrightarrow \mathfrak{A}'$: leia-se "τ é um isomorfismo entre as $\mathcal{L}$-estruturas $\mathfrak{A}$ e $\mathfrak{A}'$ "

$\mathfrak{A} \simeq \mathfrak{A}'$: leia-se "$\mathfrak{A}$ e $\mathfrak{A}'$ são isomorfas"

$\mathfrak{B} \subset \mathfrak{A}$: leia-se "$\mathfrak{B}$ é subestrutura de $\mathfrak{A}$"

$\mathfrak{B} \prec \mathfrak{A}$: leia-se "$\mathfrak{B}$ é subestrutura elementar de $\mathfrak{A}$"

$(\mathfrak{A}, A') := (\mathfrak{A}, id_{A'})$ estrutura da linguagem ampliada por constantes de $A' \subset |\mathfrak{A}|$

2 Introdução

Dados um corpo K e um inteiro positivo i, dizemos que K é um corpo $C_i(d)$ se todo polinômio homogêneo de grau total d em mais de d^i variáveis e com coeficientes em K admite uma solução não trivial em K. O corpo K é dito ainda um C_i-corpo se for $C_i(d)$ para todo $d \in \mathbb{N}^*$.

Em 1936, Chevalley mostrou que todo corpo finito é C_1 (veja [2]).

O Lema de Hensel (veja Teorema 3.2.13) nos permite provar que toda forma quadrática em mais do que $4 = 2^2$ variáveis e com coeficientes em qualquer corpo $p-$ádico $\mathbb{Q}_p$ admite solução não trivial em $\mathbb{Q}_p$. D.J. Lewis mostrou em 1952 (veja [9]) um resultado análogo para as formas cúbicas, isto é, que toda forma cúbica em mais do que $9 = 3^2$ variáveis e com coeficientes em qualquer corpo $p-$ádico $\mathbb{Q}_p$ admite solução não trivial em $\mathbb{Q}_p$. Assim, $\mathbb{Q}_p$ é $C_2(2)$ e $C_2(3)$.

Em 1963, Lang mostrou que se K é um corpo C_i então o corpo $K((X))$ das séries formais de Laurent sobre K

$$K((X)) = \left\{ \sum_{i=m}^{\infty} a_i X^i;\ m \in \mathbb{Z} \ \text{ e } \ a_i \in k \ \text{ para todo } i \geq m \right\}$$

é C_{i+1} (veja [8]), e portanto, em particular, os corpos $\mathbb{F}_p((X))$ são C_2.

Baseado na semelhança entre os corpos $\mathbb{Q}_p$ dos números $p-$ádicos e $\mathbb{F}_p((X))$ (ambos são corpos valorizados henselianos com grupo de valores $\mathbb{Z}$ e corpo de resíduos $\mathbb{F}_p$); a diferença essencial entre ambos se resume à característica: enquanto a característica de $\mathbb{F}_p((X))$ é prima, a característica de $\mathbb{Q}_p$ é zero), Artin conjecturou então que o corpo $\mathbb{Q}_p$ deveria ser também C_2.

Esta conjectura revelou-se "quase" verdadeira: em 1965, Ax e Kochen mostraram (veja [1]) que para todo grau d fixado, tem-se que é finito o conjunto dos primos p tais que $\mathbb{Q}_p$ não é $C_2(d)$. Mais precisamente:

Teorema (Ax-Kochen, 1965): Para cada grau $d \in \mathbb{N}^*$ existe uma cota n_d tal que, para todo primo $p \geq n_d$, $\mathbb{Q}_p$ é um corpo $C_2(d)$, ou seja, cada polinômio homogêneo de grau d em mais de d^2 indeterminadas reproduz o

zero de forma não-trivial.

A diferença mencionada acima entre $\mathbb{F}_p((X))$ e $\mathbb{Q}_p$ é superada quando passamos para ultraprodutos, conceito encontrado na Teoria de Modelos. A prova de Ax e Kochen faz uso também da teoria de modelos dos corpos henselianos, sendo uma aplicação do Teorema 5.1.5, cujo enunciado reproduzimos aqui:

Teorema: Sejam (F_1, σ_1) e (F_2, σ_2) corpos henselianos com corpos de restos $\overline{F_1}$ e $\overline{F_2}$ elementarmente equivalentes (na linguagem de corpos) e grupos de valores Γ_1 e Γ_2 também elementarmente equivalentes (na linguagem de grupos totalmente ordenados). Se a característica dos corpos de restos for igual a zero então (F_1, σ_1) e (F_2, σ_2) são elementarmente equivalentes (na linguagem de corpos valorizados).

O teorema de Ax e Kochen nos diz que a Conjectura de Artin é "quase" verdadeira. No caso das formas quadráticas e cúbicas (isto é, $d = 2$ e $d = 3$), temos $n_d = 0$, pelo já mencionado anteriormente. Em 1966, no entanto, Terjanian apresentou um exemplo (veja [13]) de um polinômio de grau 4 em 18 variáveis que não admite solução não trivial em $\mathbb{Q}_2$, a saber,

$$f(x_1, x_2, x_3) + f(y_1, y_2, y_3) + f(z_1, z_2, z_3) + \\ 4f(u_1, u_2, u_3) + 4f(v_1, v_2, v_3) + 4f(w_1, w_2, w_3),$$

onde

$$f(x_1, x_2, x_3) = x_1^4 + x_2^4 + x_3^4 - x_1^2x_2^2 - x_1^2x_3^2 - x_2^2x_3^2 \\ - x_1^2x_2x_3 - x_1x_2^2x_3 - x_1x_2x_3^2,$$

e portanto $\mathbb{Q}_2$ não é C_2. Com este resultado, pode-se concluir que a Conjectura de Artin não é verdadeira.

Também com ele é possível concluir que o resultado de Ax e Kochen é o melhor possível, no sentido que, para todo primo p, existem graus $d \geq 4$ para os quais $\mathbb{Q}_p$ não é $C_2(d)$, sendo que a cota 4 é de fato atingida, como nos mostra o exemplo de Terjanian.

A prova original de Ax e Kochen é até o momento a mais importante aplicação da Teoria de Mode-los à Álgebra. O objetivo deste texto é apresentar esta prova. Esta utiliza também valorizações de posto arbitrariamente grande, sugerindo que apenas o conceito de valor absoluto não seria suficiente para comprovar tal resultado.

Assim, no Capítulo 2 listamos conceitos e resultados da Teoria de Valorizações necessários para o bom entendimento desta demonstração. E, no Capítulo 3 fazemos o mesmo com relação à Teoria de Modelos para, no Capítulo 4, enunciarmos a conjuctura de Artin e provarmos o Teorema de Ax-Kochen.

As referências principais para todo este texto são [11] e [4]. Ressaltamos que, embora existam muito boas referências sobre Teoria de Valorizações, sua inclusão neste texto se justifica pelo fato de aqui listarmos apenas os resultados necessários para a prova do Teorema de Ax-Kochen.

Neste trabalho também supomos conhecidos os resultados da Teoria de Conjuntos. Uma referência para esta teoria é [5].

3 Noções da Teoria de Valorizações

Este capítulo está baseado em [4], e nele fazemos uma coletânea de nomenclaturas e resultados sobre valorizações que serão utilizados neste trabalho, e por isso alguns fatos serão mencionados sem prova. Também introduzimos os números p-ádicos $\mathbb{Q}_p$, sendo p um número primo, e consideramos também o corpo $\mathbb{F}_p((X))$ das séries formais de Laurent sobre o corpo finito $\mathbb{F}_p$ com p elementos.

Para maiores detalhes, recomendamos [7] e [12].

3.1 Valores Absolutos e Completamentos

Nesta primeira seção fazemos uma pequena introdução à teoria clássica de valores absolutos. Relembramos que em todo este texto K denota um corpo (não necessariamente de característica zero).

Definição 3.1.1 *Um valor absoluto sobre K é uma aplicação*

$$|\ |: K \to \mathbb{R},$$

satisfazendo as seguintes condições:

1. $|0| = 0$.
2. $|x| > 0$ *para todo* $x \neq 0$.
3. $|xy| = |x||y|$.
4. $|x + y| \leq |x| + |y|$,

para quaisquer $x, y \in K$.

Observamos que $|1|^2 = |1^2| = |1|$, e portanto $|1| = 1$. Similarmente, $|-1|^2 = |(-1)(-1)| = |1| = 1$, o que implica $|-1| = 1$. Daí obtemos

$$|-x| = |\ x|,$$

para todo $x \in K$. Ainda, como $|\ |$ é um homomorfismo entre os grupos multiplicativos $K^\times$ e $\mathbb{R}_+$, temos

$$|x^{-1}| = |x|^{-1},$$

para todo $x \neq 0$.

O valor absoluto que manda todo $x \neq 0$ em 1 é chamado o valor absoluto trivial em K.

Proposição 3.1.2 *O conjunto* $\{|n.1| \ ; \ n \in \mathbb{Z}\}$ *é limitado se e somente se* $|\ |$ *satisfaz a desigualdade*

$$|x + y| \leq \max\{|x|, |y|\}, \tag{1}$$

para todos $x, y \in K$.

Prova. Se $|\ |$ satisfaz (1) então, raciocinando por indução, podemos mostrar que o conjunto $\{|n.1| \ ; \ n \in \mathbb{Z}\} = \{|n.1| \ ; \ n \in \mathbb{N}\}$ é limitado por 1.

Reciprocamente, suponha que existe $C \in \mathbb{R}$ com $|n.1| \leq C$, para todo $n \in \mathbb{N}$. Então, para todos $x, y \in K$,

$$|x + y|^n = |(x + y)^n| \leq \sum_{\nu=0}^{n} \left| \binom{n}{\nu} x^\nu y^{n-\nu} \right| \leq (n + 1)C \max(|\ x|\ , |\ y|)^n.$$

Tomando raízes n-ésimas e deixando n tender ao infinito está provada a proposição.

■

Definição 3.1.3 *Um valor absoluto que satisfaz (1) é chamado não arquimediano ou ultra valor absoluto, caso contrário é chamado arquimediano.*

Da Proposição 3.1.2 obtemos:

Corolário 3.1.4 *Se* $\mathsf{car}(K) \neq 0$ *então todo valor absoluto de* K *é não arquimediano.*

Exemplo 3.1.5 *Um exemplo típico de um valor absoluto arquimediano é o chamado valor absoluto usual sobre* $\mathbb{R}$, *que é dado por*

$$|x|_0 = \begin{cases} x \text{ se } x \geq 0 \\ -x \text{ se } x \leq 0, \end{cases}$$

para todo $x \in \mathbb{R}$. *De fato,*

$$\{|n.1|_0 \ ; \ n \in \mathbb{Z}\} = \mathbb{N}$$

e portanto é ilimitado em $\mathbb{R}$.

Exemplo 3.1.6 *Para todo número primo* $p \in \mathbb{N}$, *o valor absoluto p-ádico em* $\mathbb{Q}$, *denotado por* $|\ |_p$, *é definido por:*

$$|0|_p = 0 \quad e \quad \left|p^\nu \frac{m}{n}\right|_p = e^{-\nu},$$

onde "e" é a base do logarítmo natural, $\nu \in \mathbb{Z}$ *e* $n, m \in \mathbb{Z}\backslash\{0\}$ *não são divisíveis por p. Neste caso, o conjunto*

$$\{|n.1|_p \ ; \ n \in \mathbb{Z}\} = \{e^{-\nu} \mid \nu \in \mathbb{N}\}$$

é limitado em $\mathbb{R}$, *e portanto o valor absoluto p-ádico é não-arquimediano.*

Exemplo 3.1.7 *Sendo* $k[X]$ *(onde k é um corpo) um domínio de fatoração única, podemos imitar o exemplo acima e criar um valor absoluto não arquimediano sobre o corpo das funções racionais* $K = k(X)$ *da seguinte forma: dado um polinômio irredutível* $p \in k[X]$, *definimos o valor absoluto* $|\ |_p$ *sobre* $K = k(X)$ *por:*

$$|0|_p = 0 \quad e \quad \left|p^\nu \frac{f}{g}\right|_p = e^{-\nu},$$

onde $\nu \in \mathbb{Z}$ *e* $f, g \in k[X]\backslash\{0\}$ *não são divisíveis por p. Assim, o conjunto* $\{|n.1|_p \ ; \ n \in \mathbb{Z}\}$ *é limitado por 1.*

Lema 3.1.8 *Um valor absoluto* $|\ |$ *em K define uma métrica em K se tomamos* $|x - y|$ *como a distância entre x e y para* $x, y \in K$. *Assim,*

$|\ |$ *induz uma topologia em* K, *com relação à qual todas as operações elementares em* K *são contínuas.*

Definição 3.1.9 *Se dois valores absolutos induzem a mesma topologia em* K, *eles são chamados dependentes; caso contrário, são ditos independentes.*

Proposição 3.1.10 *Sejam* $|\ |$ *e* $|\ |'$ *dois valores absolutos não triviais em* K. *Eles são dependentes se e somente se, para todo* $x \in K$,

$$|x| < 1 \text{ implica } |x|' < 1.$$

Neste caso, existe um número real $\lambda > 0$ *tal que* $|x| = (|x|')^{\lambda}$ *para todo* $x \in K$.

Prova. Para valores absolutos $|\ |$ e $|\ |'$ não triviais e dependentes em K existe $\epsilon > 0$ tal que $\{x \in K \mid |x| < \epsilon\} \subseteq \{x \in K \mid |x|' < 1\}$, uma vez que induzem a mesma topologia. Com isto, se $|x| < 1$ então existe $m \geq 1$ tal que $|x^m| = |x|^m < \epsilon$, e portanto $(|x|')^m = |x^m|' < 1$. Consequentemente $|x|' < 1$.

Reciprocamente, pela não trivialidade de $|\ |$, existe $z \in K$ com $|z| > 1$. Logo $|z^{-1}| < 1$ e assim, por hipótese, $|z^{-1}|' < 1$. Daí temos $|z|' > 1$.

Afirmação: Para todo $x \in K^{\times}$,

$$\frac{\log\ |x|}{\log\ |x|'} = \frac{\log\ |z|}{\log\ |z|'}.$$

De fato, para todos $m, n \in \mathbb{Z}$ com $n > 0$ tais que

$$\frac{m}{n} > \frac{\log\ |x|}{\log\ |z|},$$

vale $(|z|)^m > (|x|)^n$. Consequentemente

$$|x^n z^{-m}| < 1.$$

e então, pela hipótese,

$$|x^n z^{-m}|' < 1.$$

Repetindo as contas, chegamos a

$$\frac{m}{n} > \frac{\log\ |x|'}{\log\ |z|'}.$$

Está assim mostrado que

$$\frac{\log\ |x|}{\log\ |z|} \geq \frac{\log\ |x|'}{\log\ |z|'}.$$

Similarmente prova-se a desigualdade inversa, o que nos permite concluir que

$$\frac{\log\ |x|}{\log\ |z|} = \frac{\log\ |x|'}{\log\ |z|'}.$$

Definimos agora

$$\lambda = \frac{\log\ |z|}{\log\ |z|'}.$$

Daí, para todo $x \in K$,

$$\log\ |x| = \log\ |x|' \frac{\log\ |z|}{\log\ |z|'} = \lambda \log\ |x|' = \log\ (|x|')^{\lambda},$$

e portanto $|x| = (|x|')^{\lambda}$ para todo $x \in K$. A última equação implica que $|\ |$ e $|\ |'$ são dependentes.

■

Observação 3.1.11 *Com base nos axiomas de valor absoluto prova-se que* $|x| - |y| \leq |x - y|$ *e, como* $|y - x| = |x - y|$, *permutando* x *e* y *obtemos que* $||x| - |y||_0 \leq |x - y|$, *onde* $|\ |_0$ *é o valor absoluto usual nos números reais. Consequentemente, um valor absoluto* $|\ |$ *é uma aplicação uniformemente contínua de* K *com a topologia dada por* $|\ |$ *em* $\mathbb{R}$ *com a topologia usual definida por* $|\ |_0$.

O próximo teorema lida com valores absolutos independentes sobre K.

Teorema 3.1.12 (Teorema da aproximação) *Sejam* $|\ |_1, ..., |\ |_n$ *valores absolutos não triviais de* K *e dois a dois independentes. Então, fixa-*

dos $x_1, ..., x_n \in K$ *e* $\epsilon \in \mathbb{R}_+$, *existe* $x \in K$ *tal que*

$$|x - x_i|_i < \epsilon$$

para todo i.

Prova. A prova será feita em três passos, cada um deles melhorando algumas estimativas.

Afirmação 1: Para todo $1 \leq i \leq n$ existe $a_i \in K$ tal que $|a_i|_i > 1$ e $|a_i|_j < 1$ para todo $j \neq i$.

Sem perda de generalidade, fixamos $i = 1$ e escrevemos $a_1 = a$. Procedemos por indução em n.

O caso $n = 1$ é trivial pela não trivialidade de $|\ |_1$.

Para $n = 2$ a Proposição 3.1.10 implica a existência de $b, c \in K$ tais que [2]

$$|b|_1 < 1 \text{ e } |b|_2 \geq 1 \quad \text{e} \quad |c|_2 < 1 \text{ e } |c|_1 \geq 1.$$

Assim $a = b^{-1}c$ tem as propriedades desejadas.

Suponha agora que existe um $y \in K$ tal que

$$|y|_1 > 1 \quad \text{e} \quad |y|_j < 1,$$

para todo $2 \leq j \leq n-1$. Aplicando o caso $n = 2$ para $|\ |_1$ e $|\ |_n$ temos que existe $z \in K$ tal que

$$|z|_1 > 1 \quad \text{e} \quad |z|_n < 1.$$

Daí, para todo inteiro $\nu \geq 1$,

$$|zy^\nu|_1 > 1,$$

de modo que:

- se $|y|_n \leq 1$ então $|zy^\nu|_n < 1$, para todo inteiro $\nu \geq 1$. Ainda, para um inteiro $\nu \geq 1$ suficientemente grande, $|zy^\nu|_j < 1$ para todo $2 \leq j \leq n-1$,

[2] Note que para ser falsa a Proposição 3.1.10 a implicação não pode valer mesmo trocando $|\ |_1$ por $|\ |_2$.

pois $|y|_j < 1$. Assim, para um tal inteiro $\nu \geq 1$ suficientemente grande, $a = zy^\nu$ satisfaz os requisitos da afirmação;

- se $|y|_n > 1$, formamos a sequência $(w_\nu)_{\nu \in \mathbb{N}}$, onde

$$w_\nu = \frac{y^\nu}{1+y^\nu} = \frac{1}{\frac{1}{y^\nu}+1}.$$

As propriedades usuais dos número reais e a Observação 3.1.11 implicam que

$$\lim_{\nu \to \infty} |w_\nu|_j = 0 \text{ para } 2 \leq j \leq n-1.$$

De fato,

$$|w_\nu|_j = \left| \frac{1}{\frac{1}{y^\nu}+1} \right|_j = \frac{1}{\left|\frac{1}{y^\nu}+1\right|_j} \overset{\text{Obs. 3.1.11}}{\leq} \frac{1}{\left|\left|\frac{1}{y^\nu}\right|_j + 1\right|_0} = \frac{1}{\frac{1}{|y|_j^\nu}+1}$$

que tende a zero pois $|y|_j < 1$.

Também

$$\lim_{\nu \to \infty} |w_\nu - 1|_j = 0 \text{ para } j = 1 \text{ e } j = n.$$

pois

$$|w_\nu - 1|_j = \left| \frac{y^\nu}{1+y^\nu} - 1 \right|_j = \left| \frac{1}{1+y^\nu} \right|_j = \frac{1}{|1+y^\nu|_j} \overset{\text{Obs. 3.1.11}}{\leq} \frac{1}{1+|y|_j^\nu}$$

que tende a zero pois $|y|_1 > 1$ e $|y|_n > 1$.

Consequentemente

$$\lim_{\nu \to \infty} |zw_\nu|_j = 0 \text{ para } 2 \leq j \leq n-1$$

e

$$\lim_{\nu \to \infty} |zw_\nu|_j = |z|_j \text{ para } j = 1 \text{ e } j = n.$$

Portanto, para um ν suficientemente grande, o elemento $a = zw_\nu$ tem as propriedades requisitadas.

Afirmação 2: Para todo número real $\epsilon > 0$ e todo i tal que $1 \leq i \leq n$ existe $c_i \in K$ tal que $|c_i - 1|_i < \epsilon$ e $|c_i|_j < \epsilon$ para todo $j \neq i$.

Como antes, podemos supor $i = 1$. Seja $a \in K$ satisfazendo as condições da Afirmação 1 para $i = 1$:

$$|a|_1 > 1 \quad \text{e} \quad |a|_j < 1, \quad \text{para todo } j \neq 1.$$

Então a sequência

$$\left| \frac{a^\nu}{1 + a^\nu} \right|_j$$

converge para 1 para $j = 1$, e converge para 0 para $j > 1$. Logo para ν suficientemente grande,

$$c_1 = \frac{a^\nu}{1 + a^\nu}$$

tem a propriedade requerida.

Afirmação 3: De acordo com a Afirmação 2 acima, existem elementos $c_1, ..., c_n \in K$ tais que c_i está próximo de 1 em $|\ |_i$ e para todo $j \neq i$ temos c_i próximo de 0 em $|\ |_j$.

O elemento $x = c_1 x_1 + ... + c_n x_n$ está arbitrariamente próximo de x_i em $|\ |_i$ para todo $i = 1, ..., n$, e portanto satisfaz as condições do teorema.

∎

Podemos também considerar o completamento de K com respeito a um valor absoluto $|\ |$.

Definição 3.1.13 *Uma sequência $(x_n)_{n \in \mathbb{N}}$ de elementos de K é dita uma sequência de Cauchy com respeito ao valor absoluto $|\ |$ de K se, para todo $\epsilon > 0$, existe $N \in \mathbb{N}$ tal que*

$$n, m > N \Rightarrow |x_n - x_m| < \epsilon.$$

O corpo K é dito completo com respeito ao valor absoluto $|\ |$ se toda sequência de Cauchy de elementos de K é convergente.

O valor absoluto trivial faz qualquer corpo completo.

No próximo teorema mostramos que todo corpo K munido de um valor absoluto $|\ |$ não trivial pode ser imerso densamente em um corpo completo $\widehat{K}$ munido de um valor absoluto $\widehat{|\ |}$ que estende o de K.

Definição 3.1.14 *Um subconjunto A de um espaço métrico (M, d) é dito denso em M se para todo $x \in M$ e $\epsilon > 0$ existe $y \in A$ tal que $d(x, y) < \epsilon$.*

É fácil ver que $\mathbb{Q}$ não é completo com relação ao valor absoluto usual $|\ |_0$; também não o é com relação ao valor absoluto p-ádico $|\ |_p$: de fato, a sequência $(x_n)_{n\in\mathbb{N}}$ de números racionais dada por

$$x_n = 1 + p + ... + p^n$$

é de Cauchy, pois, dado $\epsilon > 0$, escolhendo $N \in \mathbb{N}$ tal que $N + 1 > \ln \frac{1}{\epsilon}$, temos

$$m > n > N \Rightarrow |x_m - x_n|_p = |p^{n+1} + ... + p^m|_p = e^{-(n+1)} < e^{-(N+1)} < \epsilon.$$

Agora, se a sequência convergisse, digamos, para o racional a/b onde $mdc(a, b) = 1$, então, como

$$x_n = \frac{p^{n+1} - 1}{p - 1},$$

teríamos

$$\begin{aligned}
\left|\frac{a}{b} - x_n\right|_p &= \left|\frac{a}{b} - \frac{p^{n+1} - 1}{p - 1}\right|_p \\
&= \left|\frac{p^{n+1}}{p - 1} - \frac{a}{b} - \frac{1}{p - 1}\right|_p \overset{\text{Obs. 3.1.11}}{\geq} \\
&\geq \left|\left|\frac{p^{n+1}}{p - 1}\right|_p - \underbrace{\left|\frac{a}{b} + \frac{1}{p - 1}\right|_p}_{\text{constante: } c}\right|_0 = |n + 1 - c|_0 ,
\end{aligned}$$

o que não converge a zero. Portanto chegamos numa contradição.

No entanto encontraremos $\mathbb{Q}$ denso dentro de um correspondente completamento, chamado *corpo dos números p-ádicos*:

Teorema 3.1.15 *Se K é um corpo com valor absoluto não trivial $|\ |$, então existe um corpo $\widehat{K}$ completo com respeito a um valor absoluto $\widehat{|\ |}$ e uma imersão $i : K \to \widehat{K}$ com $|x| = \widehat{|i(x)|}$, para todo $x \in K$. Além disso, $i(K)$ é denso em $\widehat{K}$.*

Ainda, se $(\widehat{K}', i')$ é outro tal par de corpo completo e de imersão, então existe um único isomorfismo contínuo

$$\varphi : \widehat{K} \to \widehat{K}'$$

preservando o valor absoluto e fazendo o seguinte diagrama comutar.

$$\begin{array}{ccc} \widehat{K} & \xrightarrow{\varphi} & \widehat{K}' \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle i'} \\ K & \xrightarrow{id} & K \end{array}$$

Prova. Seja $\mathcal{C}$ o conjunto de todas as sequências de Cauchy $(x_n)_{n\in\mathbb{N}}$ de elementos de K. Definindo a soma e a multiplicação de sequências como sendo a sequência obtida quando fazemos estas operações termo a termo, é fácil convencer-se que $\mathcal{C}$ é um anel comutativo com unidade $(1)_{n\in\mathbb{N}}$. Afirmamos que o conjunto

$$\mathcal{N} = \left\{ (x_n)_{n\in\mathbb{N}} \mid \lim_{n\to\infty} x_n = 0 \right\}$$

é um ideal de $\mathcal{C}$. De fato, é claro, por (4) da Definição 3.1.1, que $\mathcal{N}$ é fechado para a soma. Para verificar a propriedade multiplicativa tome $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}$. Então existe um $N \in \mathbb{N}$ tal que

$$|\ a_n - a_{N+1}| < 1 \text{ para todo } n > N.$$

Tomando agora $(b_n)_{n\in\mathbb{N}} \in \mathcal{N}$ e $\epsilon > 0$, deve existir, para este N fixado, um $M \in \mathbb{N}$ tal que

$$n > M \Rightarrow |\ b_n| < \frac{\epsilon}{1 + |\ a_{N+1}|}. \tag{2}$$

Afirmamos que $|a_n b_n| < \epsilon$ para todo $n > \max\{N, M\}$, e portanto $(a_n b_n)_{n\in\mathbb{N}} \in \mathcal{N}$. De fato,

$$1 > |\ a_n - a_{N+1}| > |a_n| - |a_{N+1}|$$

e portanto

$$|a_{N+1}| + 1 > |a_n|$$

donde

$$|a_n b_n| < |b_n|\ \ (|a_{N+1}| + 1) < \frac{\epsilon\,(|a_{N+1}| + 1)}{1 + |\ a_{N+1}|} = \epsilon.$$

Em particular, a implicação (2) nos mostra também que toda sequência de $\mathcal{N}$ tem uma cota superior.

Afirmação 1: Toda sequência de $\mathcal{C}\backslash\mathcal{N}$ possui uma cota inferior positiva.

De fato, se isto não fosse verdade, para uma certa sequência $(a_n)_{n\in\mathbb{N}}$ neste conjunto, para todo número real $\eta > 0$ e todo $N \in \mathbb{N}$, teríamos $|a_m| < \eta$ para algum $m > N$. Por ser sequência de Cauchy, dado $\epsilon > 0$ existe $M \in \mathbb{N}$ tal que

$$p, q > M \ \Rightarrow\ |a_p - a_q| < \frac{\epsilon}{2}.$$

Mas então (pondo $\eta = \frac{\epsilon}{2}$), existe um $m > M$ com $|\ a_m| < \epsilon/2$. Daí, para todo $p > M$ temos

$$|\ a_p| = |a_p - a_m + a_m| \leq |a_p - a_m| + |a_m| < \epsilon,$$

o que contradiz a hipótese de $(a_n)_{n\in\mathbb{N}} \notin \mathcal{N}$.

Assim, para toda sequência $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}\backslash\mathcal{N}$ devem existir $\eta > 0$ e $M \in \mathbb{N}$ satisfazendo

$$n > M \Rightarrow |\ a_n| > \eta. \tag{3}$$

Afirmação 2: $\mathcal{N}$ é um ideal maximal de $\mathcal{C}$.

Para tal, basta-nos mostrar que toda sequência $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}\backslash\mathcal{N}$ quando unida a $\mathcal{N}$ gera todo o anel $\mathcal{C}$.

De fato, inicialmente observamos que a sequência $(c_n)_{n\in\mathbb{N}}$ dada por

$$c_n = 1 \text{ para todo } n \in \{1, ..., M\} \text{ e } c_n = a_n^{-1} \text{ para todo } n > M,$$

sendo M dado por (3), é uma sequência de Cauchy, pois, dados $\epsilon > 0$ e $\eta > 0$, existe $N \in \mathbb{N}$ tal que $|a_p - a_q| < \eta^2\epsilon$ para todo $p, q > N$, pois $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}$. Portanto, se $n > \max\{N, M\}$ vale então

$$|c_p - c_q| = \left|\frac{1}{a_p} - \frac{1}{a_q}\right| = \frac{|a_p - a_q|}{|a_p||a_q|} < \eta^{-2}\eta^2\epsilon = \epsilon.$$

Mostramos com isto também que se $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}\backslash\mathcal{N}$ então existe $(c_n)_{n\in\mathbb{N}}$ tal que

$$(a_n)_{n\in\mathbb{N}}(c_n)_{n\in\mathbb{N}} - (1)_{n\in\mathbb{N}} \in \mathcal{N}.$$

Como $\mathcal{N}$ é ideal maximal, o quociente

$$\widehat{K} = \mathcal{C}/\mathcal{N}$$

é um corpo.

A aplicação $i : K \to \widehat{K}$, definida por $x \mapsto (x)_{n\in\mathbb{N}} + \mathcal{N}$ (classe da sequência constante igual a x), define uma imersão de K em $\widehat{K}$.

Resta-nos agora construir em $\widehat{K}$ um valor absoluto que estende $|\ |$ e mostrar a densidade de K em $\widehat{K}$.

Pela Observação 3.1.11, para cada sequência $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}$ temos uma sequência $(|a_n|)_{n\in\mathbb{N}}$ de Cauchy de números reais (portanto convergente com relação ao valor absoluto usual), e para $(a_n)_{n\in\mathbb{N}} \in \mathcal{N}$ a sequência $(|a_n|)_{n\in\mathbb{N}}$ tem limite igual a 0. Assim, definindo em $\widehat{K}$ o valor absoluto da classe $\zeta = (a_n)_{n\in\mathbb{N}} + \mathcal{N}$ por

$$\widehat{|\zeta|} = \lim_{n\to\infty} |a_n|,$$

vemos que ele é independente do representante escolhido para a classe. Observando as propriedades de limites e de valor absoluto, verifica-se que

$\widehat{|\ |}$ é um valor absoluto em $\widehat{K}$ que estende $|\ |$ em K: de fato, dados $x \in K$ e $\zeta = (x)_{n\in\mathbb{N}} + \mathcal{N}$, temos

$$\widehat{|\zeta|} = \lim_{n\to\infty} |x| = |x|.$$

Provamos agora que $i(K)$ é denso em $\widehat{K}$ com respeito ao valor absoluto $\widehat{|\ |}$. Dados $\zeta \in \widehat{K}$, $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}$ um representante de ζ e $\epsilon > 0$, escolhemos $N \in \mathbb{N}$ satisfazendo

$$p, q > N \Rightarrow |a_p - a_q| < \epsilon.$$

Daí, para para todo $n > N$,

$$\widehat{|\zeta - i(a_n)|} = \lim_{p\to\infty} |a_p - a_n| < \epsilon.$$

Logo, para $n > N$, o elemento $i(a_n)$, que é a classe da sequência constante igual a a_n, está $\epsilon-$próximo de ζ na métrica $\widehat{|\ |}$, o que comprova a densidade de $i(K)$ em $\widehat{K}$.

Também a última desigualdade nos mostra que, dada a sequência $(a_n)_{n\in\mathbb{N}}$ com $a_n \in K$, a sequência $(i(a_n))_{n\in\mathbb{N}}$ converge para $\zeta = (a_n)_{n\in\mathbb{N}} + \mathcal{N}$.

Com isto vamos verificar que $\widehat{K}$ é completo. Seja $(\xi_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy em $\widehat{K}$. Como $i(K)$ é denso em $\widehat{K}$, podemos tomar para cada n um $x_n \in K$ com

$$\widehat{|\xi_n - i(x_n)|} < \frac{1}{n}.$$

Para todo número real $\epsilon > 0$ existe $N \in \mathbb{N}$ tal que

$$p, q > N \Rightarrow \frac{1}{p} < \frac{\epsilon}{3}, \quad \frac{1}{q} < \frac{\epsilon}{3}, \quad \widehat{|\xi_p - \xi_q|} < \frac{\epsilon}{3}.$$

Consequentemente, para todo $p, q > N$,

$$|x_p - x_q| = \widehat{|i(x_p) - i(x_q)|} \leq \widehat{|i(x_p) - \xi_p|} + \widehat{|\xi_p - \xi_q|} + \widehat{|\xi_q - i(x_q)|} < \epsilon,$$

e então $(x_n)_{n\in\mathbb{N}} \in \mathcal{C}$. Tomando $\xi = (x_n)_{n\in\mathbb{N}} + \mathcal{N} \in \widehat{K}$ e relembrando que $\lim_{n\to\infty} i(x_n) = \xi$, obtemos para $\epsilon > 0$ e um n suficientemente grande

$$\widehat{|\xi - \xi_n|} \leq \widehat{|\xi - i(x_n)|} + \widehat{|i(x_n) - \xi|} < \epsilon,$$

ou seja, $(\xi_n)_{n\in\mathbb{N}}$ converge para ξ. Isto prova que $\widehat{K}$ é completo.

Finalmente, provemos a unicidade do completamento. Se $(\widehat{K}', \widehat{|\ |}')$ é um par com as mesmas propriedades de $(\widehat{K}, \widehat{|\ |})$ então para toda $\xi = (a_n)_{n\in\mathbb{N}} + \mathcal{N} \in \widehat{K}$, a sequência $(i'(a_n))_{n\in\mathbb{N}}$ é de Cauchy em $\widehat{K}'$. Se ξ' é o limite desta sequência em $\widehat{K}'$, definimos $\varphi : \widehat{K} \to \widehat{K}'$ por $\varphi(\xi) = \xi'$.

Da unicidade do limite segue que φ está bem definida. Como $i'(K)$ é denso em $\widehat{K}'$, φ é sobrejetiva. Da hipótese de i e i' serem homomorfismos e novamente pela unicidade do limite temos que φ é um homomorfismo. Por argumentos puramente topológicos φ é contínua, e claramente o diagrama do teorema comuta.

Por fim, sendo um homomorfismo não trivial de corpos, temos que φ é injetora.

■

Definição 3.1.16 *O par $(\widehat{K}, \widehat{|\ |})$ construído no teorema acima é dito o completamento de $(K, |\ |)$.*

3.2 Corpos Completos não Arquimedianos

Nesta seção tratamos apenas de valores absolutos $|\ |$ sobre um corpo K que são não triviais e não arquimedianos. Entre as propriedade apresentadas está o Lema de Hensel (veja o Teorema 3.2.13).

Na próxima seção generalizamos a noção de valor absoluto não arquimediano definindo valorização. Para esta generalização é mais conveniente usar a representação "aditiva" do valor absoluto $|\ |$. Por isto definimos

Definição 3.2.1 *A valorização (naturalmente) associada a um valor absoluto $|\ |$ sobre um corpo K não trivial e não arquimediano é a aplicação*

$v : K \to \mathbb{R} \cup \{\infty\}$ *dada por*

$$v(x) := \begin{cases} \infty, \text{ se } x = 0 \\ -\ln|x|, \text{ se } x \neq 0 \end{cases}$$

Desta forma, os axiomas de valor absoluto não arquimediano (veja Definição 3.1.1) são reescritos, para todo $x, y \in K$, *como:*

1. $v(x) \in \mathbb{R}$ *para* $x \neq 0$ *e* $v(0) = \infty$.
2. $v(xy) = v(x) + v(y)$.
3. $v(x+y) \geq \min\{v(x), v(y)\}$,

sendo ∞ *um símbolo para a valorização em* 0 *que satisfaz o seguinte axioma: para todo* $\gamma \in \mathbb{R}$,

$$\infty = \infty + \infty = \gamma + \infty = \infty + \gamma. \tag{4}$$

Exemplo 3.2.2 *A valorização associada ao valor absoluto trivial é a aplicação identicamente nula:* $v(x) = 0$ *para todo* x *não nulo em* K.

Exemplo 3.2.3 *No caso do valor absoluto p-ádico* $|\ |_p$ *em* $\mathbb{Q}$ *denotando por* v_p *a correspondente valorização, temos (com as mesmas notações utilizadas no Exemplo 3.1.6)*

$$v_p\left(p^\nu \frac{m}{n}\right) = -\ln|p^\nu \frac{m}{n}| = -\ln e^{-\nu} = \nu,$$

que é denominada valorização p-ádica em $\mathbb{Q}$.

Exemplo 3.2.4 *Procedemos similarmente ao Exemplo 3.1.7, definindo a valorização* $p(X)-$*ádica em* $K(X)$, *denotada por* v_p. *Note que, no caso em que* $k = \mathbb{C}$ *e* $p = X$, *a função* v_p *aplicada a uma função racional* ρ *nos dá precisamente a "ordem" de* ρ *em* 0, *ou seja, se*

$$v_p(\rho) = \nu > 0$$

então ρ *tem um zero de ordem* ν *em* 0, *e se* $v_p(\rho) = \nu < 0$ *então* ρ *tem um pólo de ordem* ν *em* 0.

Salientamos que na Definição 3.2.1 somente a estrutura aditiva de $\mathbb{R}$ junto com sua ordem foram u-sadas. No próximo capítulo generalizamos esta definição, definindo valorizações de Krull, requerendo apenas que v tome os valores em um grupo abeliano totalmente ordenado.

Convenção e Notação: Aqui fazemos um pequeno abuso de linguagem passando a nos referir à função v também pelo nome de valor absoluto. Assim, no resto desta seção, v denotará sempre um valor absoluto não arquimediano (com a notação aditiva).

Dado um valor absoluto não arquimediano v em K, o conjunto

$$\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$$

é um subanel de K. De fato, como $|-y| = |y|$, temos, para todo $x, y \in \mathcal{O}_v$,

$$v(x \pm y) \geq \min\{v(x), v(\pm y)\} \geq 0 \quad \text{e} \quad v(xy) = v(x) + v(y) \geq 0.$$

e portanto $x \pm y, xy \in \mathcal{O}_v$. Ainda, como $|x^{-1}| = |x|^{-1}$, temos

$$v(x^{-1}) = -v(x);$$

daí concluímos que

$$x \text{ é uma unidade em } \mathcal{O}_v \text{ se e somente se } v(x) = 0,$$

e que, para todo $x \in K^\times$,

$$x \in \mathcal{O}_v \quad \text{ou} \quad x^{-1} \in \mathcal{O}_v.$$

Definição 3.2.5 *Um subanel $\mathcal{O}$ de K que satisfaz*

$$x \in \mathcal{O} \text{ ou } x^{-1} \in \mathcal{O}$$

para todo $x \in K^\times$ é chamado um anel de valorização de K.

Logo $\mathcal{O}_v$ é um anel de valorização de K. Facilmente mostra-se que

$$\mathcal{M}_v := \{x \in K \mid v(x) > 0\}$$

é um ideal de $\mathcal{O}_v$. Como $\mathcal{M}_v$ é ideal e consiste exatamente das não unidades de $\mathcal{O}_v$, ele é o seu único ideal maximal. Assim $\mathcal{O}_v$ é um anel local.

Definição 3.2.6 *O corpo da classe de resíduos*

$$\overline{K_v} := \mathcal{O}_v/\mathcal{M}_v$$

é chamado o corpo de resíduos de v.

Como habitual, a classe de resíduos de a em $\mathcal{O}_v$ é denotada por $\overline{a}$.

Também não é difícil convercer-se que $v(K^\times)$ é um grupo aditivo.

Definição 3.2.7 *O grupo $v(K^\times)$ associado a um valor absoluto v de um corpo K é chamado o grupo de valores de v.*

Determinamos agora o anel de valorização, o ideal maximal e o corpo de resíduos no caso dos exemplos mencionados acima

Exemplo 3.2.8 *Note que v é o valor absoluto trivial se e somente se $\mathcal{O}_v = K$, e portanto também $\overline{K_v} = K$.*

Exemplo 3.2.9 *No caso da valorização p-ádica $v = v_p$ de $\mathbb{Q}$, pelo Exemplo 3.2.3, vemos que*

$$\mathcal{O}_{v_p} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z};\ a \text{ e } b \text{ relativamente primos e } b \text{ não é divisível por } p\right\}$$

e

$$\mathcal{M}_{v_p} = \left\{p\frac{a}{b} \mid a, b \in \mathbb{Z},\ \text{relativamente primos, e } b \text{ não é divisível por } p\right\}.$$

Claramente $\mathcal{O}_{v_p}$ é a localização $\mathbb{Z}_{(p)}$ do anel $\mathbb{Z}$ pelo ideal primo $(p) = p\mathbb{Z}$ e $\mathcal{M}_{v_p}$ é o ideal $p\mathbb{Z}_{(p)}$ de $\mathbb{Z}_{(p)}$. Logo o corpo de resíduos $\overline{K}_{v_p}$ é isomorfo ao corpo primo $\mathbb{F}_p$.

Exemplo 3.2.10 *Para o Exemplo 3.1.7 temos como anel de valorização a localização $k[X]_{(p)}$ de $k[X]$ pelo ideal primo $(p) = p.k[X]$ e $p.k[X]_{(p)}$ é o ideal maximal. O corpo de resíduos é canonicamente isomorfo a $k[X]/(p)$.*

Ainda não fizemos uso do fato de $v(K^\times)$ ser um subgrupo do grupo aditivo dos reais. A seguinte propriedade é necessaria para o Lema de Hensel:

Lema 3.2.11 *Se v é um valor absoluto de um corpo K então, para quaisquer $x, y \in K$,*

$$v(x) < v(y) \Rightarrow v(x+y) = v(x)$$

Prova. Se fosse $v(x+y) > v(x)$, então teríamos

$$v(x) = v((x+y)-y) \geq \min\{v(x+y), v(-y)\} > v(x),$$

uma contradição.

∎

Como corolário temos

Corolário 3.2.12 *Se $x_1, ..., x_n \in K$ são tais que o mínimo do conjunto $\{v(x_1), ..., v(x_n)\}$ é atingido para um único $v(x_i)$, então $v(x_1 + ... + x_n) = v(x_i)$.*

Prova. Sem perda de generalidade tomamos $i = 1$. Vale então

$$\begin{aligned} v(x_2 + ... + x_n) &\geq \min\{v(x_2), v(x_3 + ... + x_n)\} \\ &\geq ... \geq \min\{v(x_2), ..., v(x_n)\} > v(x_1), \end{aligned}$$

e o Lema acima implica o Corolário.

∎

Lembramos que, para cada $b \in \mathcal{O}_v$,

$\overline{b} = \overline{0}$ se e somente se $v(b) > 0$ e $\overline{b} \neq \overline{0}$ se e somente se $v(b) = 0$.

Um fato que também é útil se ter em mente é que se v é a valorização naturalmente associada ao valor absoluto $|\ |$ então

$$\lim_{n\to\infty}|a_n - a| = 0 \Leftrightarrow \lim_{n\to\infty} v(a_n - a) = \infty,$$

o que nos diz que ao nos aproximarmos de 0 por $|\ |$ nos aproximamos de ∞ por v, e vice-versa.

Agora chegamos a uma propriedade importante de um corpo K completo com respeito a um valor absoluto não arquimediano e não-trivial v. Estamos denotando por $f\,'(X)$ a derivada formal de $f(X)$. É aqui que fazemos uso pela primeira vez do fato de $v(K^\times)$ ser um subgrupo do grupo aditivo dos reais.

Teorema 3.2.13 (Lema de Hensel) [3] *Seja K um corpo completo com respeito a um valor absoluto não-trivial e não arquimediano v. Seja $f \in \mathcal{O}_v[X]$ um polinômio, e seja $a_0 \in \mathcal{O}_v$ tal que*

$$v(f(a_0)) > 2v(f\,'(a_0)) = v([f\,'(a_0)]^2).$$

Então existe um $a \in \mathcal{O}_v$ com $f(a) = 0$ e $v(a_0 - a) > v(f\,'(a_0))$.

Prova. Vamos provar o teorema construindo uma sequência de Cauchy conveniente que converge para uma raiz a de f, usando que todo polinômio f é uma aplicação contínua (consequência do Lema 3.1.8 e da Definição 3.1.16).

Seja

$$b_0 = f\,'(a_0) \in \mathcal{O}_v.$$

Temos $b_0 \neq 0$ pois por hipótese

$$\infty \geq v(f(a_0)) > 2v(f\,'(a_0)) = v(b_0^2),$$

de modo que $v(b_0) \neq \infty$.

[3] Na Seção 3.6 este resultado será mais motivado, numa situação mais geral de corpos valorizados.

Escolhemos $\epsilon > 0$ tal que

$$v(f(a_0)) \geq v(b_0^2) + \epsilon,$$

que existe, por hipótese. Então, pondo

$$c_0 = f(a_0)/b_0^2 \in K,$$

temos que

$$f(a_0) = b_0^2 c_0 \quad \text{e} \quad v(c_0) \geq \epsilon > 0;$$

em particular, $c_0 \in \mathcal{O}_v$.

Definimos

$$a_1 := a_0 - b_0 c_0 \in \mathcal{O}_v.$$

Usando o fato que f é um polinômio com coeficientes em $\mathcal{O}_v$ e que $a_0, b_0, c_0 \in \mathcal{O}_v$, existe $d_0 \in \mathcal{O}_v$ tal que

$$\begin{aligned} f(a_1) &= f(a_0 - b_0 c_0) \\ &= f(a_0) - b_0 c_0 f'(a_0) + b_0^2 c_0^2 d_0 \overset{f(a_0)=b_0^2 c_0 \text{ e } f'(a_0)=b_0}{=} b_0^2 c_0^2 d_0. \end{aligned}$$

Disto segue

$$v(f(a_1)) = v(b_0^2 c_0^2 d_0) = v(b_0^2) + 2v(c_0) + v(d_0) \overset{v(c_0)\geq\epsilon \text{ e } d_0\in\mathcal{O}_v}{\geq} v(b_0^2) + 2\epsilon. \quad (5)$$

Aplicando um procedimento similar para f', segue que existe $b \in \mathcal{O}_v$ tal que

$$f'(a_1) = f'(a_0 - b_0 c_0) = f'(a_0) - b_0 c_0 b \overset{f'(a_0)=b_0}{=} b_0(1 - c_0 b) =: b_1.$$

Então

$$v(b_1) = v(b_0), \quad (6)$$

pois

$$v(c_0) > 0, \ b \in \mathcal{O}_v \ \Rightarrow \ v(c_0 b) > 0$$

e portanto

$$v(1 - c_0 b) = \min\{v(1), v(-c_0 b)\} = 0.$$

Tomando

$$c_1 := f(a_1)/b_1^2 \tag{7}$$

obtemos

$$f(a_1) = b_1^2 c_1 \quad \text{com} \quad c_1 \in K,$$

e então por (7) vemos que

$$v(c_1) = v\left(\frac{f(a_1)}{b_1^2}\right) = v(f(a_1)) - 2v(b_1) \overset{(6)}{=} v(f(a_1)) - 2v(b_0) \overset{(5)}{\geq} 2\epsilon.$$

Repetindo o argumento acima com ϵ, b_0 e a_1 substituídos por $2\epsilon, b_1$ e

$$a_2 = a_1 - b_1 c_1,$$

respectivamente, chegamos à existência de b_2 com $f'(a_2) = b_2$ tal que

$$v(b_2) = v(b_0) \quad \text{e} \quad f(a_2) = b_2^2 c_2$$

para algum c_2 com

$$v(c_2) \geq 4\epsilon.$$

Iterando este processo encontramos uma sequência

$$a_{n+1} = a_n - b_n c_n. \tag{8}$$

onde

$$f'(a_{n+1}) = b_{n+1}; \tag{9}$$
$$v(b_{n+1}) = v(b_0); \tag{10}$$
$$f(a_{n+1}) = b_{n+1}^2 c_{n+1}; \tag{11}$$
$$v(c_{n+1}) \geq 2^{n+1}\epsilon.$$

Afirmamos que a sequência $(a_n)_{n\in\mathbb{N}}$ é de Cauchy uma vez que $2^n\epsilon \to \infty$

quando $n \to \infty$. De fato, para $m \leq n$

$$\begin{aligned} v(a_n - a_m) &= v\left(\sum_{i=m}^{n-1}(a_{i+1} - a_i)\right) \\ &\geq \min_{m\leq i\leq n}\{v(a_{i+1} - a_i)\} \\ &\overset{(8)}{=} \min_{m\leq i\leq n}\{v(-b_i c_i)\} \\ &= \min_{m\leq i\leq n}\{v(b_i) + v(c_i)\} \\ &\geq v(b_0) + 2^m\epsilon. \end{aligned} \tag{12}$$

Seja

$$a = \lim_{n\to\infty} a_n$$

que pertence a K pois K é completo.

Como polinômios são aplicações contínuas, temos que

$$f(a) = \lim_{n\to\infty} f(a_n), \tag{13}$$

$$f'(a) = \lim_{n\to\infty} f'(a_n) \overset{(9)}{=} \lim_{n\to\infty} b_n. \tag{14}$$

Como

$$v(f(a_n)) \overset{(11)}{=} v(b_n^2) + v(c_n) \overset{(10)}{=} v(b_0^2) + v(c_n) \geq 2^n\epsilon,$$

para todo $n \in \mathbb{N}$, o limite em (13) tem valor ∞, ou seja,

$$f(a) = 0.$$

Do limite em (14) podemos deduzir que

$$v(f'(a)) = v(b_0).$$

De fato, como $b_0 \neq 0$, para $\delta > v(b_0)$, existe n tal que

$$v(f'(a) - b_n) > \delta > v(b_0) \overset{(10)}{=} v(b_n).$$

Como já observamos antes, esta desigualdade implica

$$v(f'(a)) = v\left((f'(a) - b_n) + b_n\right) = v(b_n) \overset{(10)}{=} v(b_0).$$

Segue de (12) que, para um n suficientemente grande,

$$\begin{aligned} v(a - a_0) &= v((a - a_n) + (a_n - a_0)) \\ &\geq \min\{v(a - a_n), v(a_n - a_0)\} \\ &= v(a_n - a_0) = v(b_0) + \epsilon, \end{aligned}$$

Consequentemente $v(a - a_0) > v(b_0) = v(f'(a_0))$, como queríamos.

■

Observação 3.2.14 *Salientamos que na demonstração acima, se $v(f(a_0)) = \infty$ então basta-nos tomar $a = a_0$.*

Definição 3.2.15 *Para um polinômio $f \in \mathcal{O}_v[X]$ escrito como*

$$f = c_0 + c_1 X + ... + c_n X^n$$

chamamos

$$\overline{f} = \overline{c_0} + \overline{c_1} X + ... + \overline{c_n} X^n$$

o polinômio residual de f.

O próximo corolário é uma consequência do Lema de Hensel:

Corolário 3.2.16 *Seja K um corpo completo com respeito a um valor absoluto não-trivial e não arquimediano v. Se $f \in \mathcal{O}_v[X]$ e $\overline{f}$ tem um zero simples $\overline{a_0}$ no corpo de resíduos $\overline{K}_v$, ou seja, $\overline{f}(\overline{a_0}) = \overline{0}$ e $\overline{f}'(\overline{a_0}) \neq \overline{0}$, então f tem um zero $a \in \mathcal{O}_v$ tal que $\overline{a} = \overline{a_0}$.*

Prova. As hipóteses $\overline{f}(\overline{a_0}) = \overline{0}$ e $\overline{f}'(\overline{a_0}) \neq \overline{0}$ significam

$$v(f(a_0)) > 0 \quad \text{e} \quad v(f'(a_0)) = 0,$$

e portanto

$$v(f(a_0)) > 2v(f'(a_0)).$$

O Lema de Hensel nos garante então que existe $a \in \mathcal{O}_v$ tal que

$$f(a) = 0 \quad \text{e} \quad v(a_0 - a) > v(f'(a_0)) = 0,$$

e portanto $\overline{a} = \overline{a_0}$.

■

Observação 3.2.17 *A prova do Lema de Hensel (Teorema 3.2.13) claramente mostra que, nas hipóteses deste teorema (ou do Corolário 3.2.16), a sequência $(f(a_n))_{n\in\mathbb{N}}$ converge para 0. No entanto, a mesma demosntração nos permite afirmar que sem a hipótese da completude de K ainda vale*

Corolário 3.2.18 *Seja v um valor absoluto não arquimediano em um corpo K não necessariamente completo. Então, para todo $f \in \mathcal{O}_v[X]$, se $\overline{f}$ tem um zero simples em $\overline{K_v}$, então $f(K)$ se aproxima de 0.*

Consideremos agora o completamento $(\widehat{K}, \widehat{v})$ de um corpo com respeito a um valor absoluto não arquimediano v de K (construído no Teorema 3.1.15), mas agora usando a notação aditiva para valores absolutos. A densidade de K em $\widehat{K}$ tem a seguinte consequência importante.

Teorema 3.2.19 *Denotemos por $\mathcal{O}_{\widehat{v}}$, $\overline{K_{\widehat{v}}}$ e $\mathcal{O}_v$, $\overline{K}_v$ os anéis de valorização e os corpos de resíduos de $\widehat{v}$ e v, respectivamente. Então os corpos de resíduos $\overline{K}_v$ e $\overline{K_{\widehat{v}}}$, assim como os grupos de valores $v(K^\times)$ e $\widehat{v}(\widehat{K}^\times)$ são canonicamente isomorfos.*

Prova. Segue da construção feita no Teorema 3.1.15 que

$$\mathcal{O}_{\widehat{v}} \cap K = \mathcal{O}_v \text{ e } \mathcal{M}_{\widehat{v}} \cap \mathcal{O}_v = \mathcal{M}_v,$$

onde $\mathcal{M}_{\widehat{v}}$ e $\mathcal{M}_v$ são os respectivos ideais maximais. Logo a aplicação que manda a classe de resíduos de $a \in \mathcal{O}_v$ na classe de resíduos $\overline{a} \in \mathcal{O}_{\widehat{v}}/\mathcal{M}_{\widehat{v}}$ está

bem definida. Claramente esta aplicação é um homomorfismo não trivial de corpos, e portanto é uma aplicação injetora. Falta ver que é sobrejetora.

Para todo $x \in \mathcal{O}_{\widehat{v}}$, o conjunto $x + \mathcal{M}_{\widehat{v}}$ é uma vizinhança aberta de x. De fato, ela consiste de todos os elementos z tais que

$$\widehat{v}(z - x) > 0$$

ou seja, em termos de valor absoluto,

$$\widehat{|z - x|} < 1.$$

Pela densidade de K em $\widehat{K}$, o conjunto $(x + \mathcal{M}_{\widehat{v}}) \cap K$ é não vazio. Cada $y \in (x + \mathcal{M}_{\widehat{v}}) \cap K$ é um elemento de K tal que $y - x \in \mathcal{M}_{\widehat{v}}$ e portanto

$$\widehat{v}(y - x) > 0;$$

Mas

$$\widehat{v}(y - x) \geq \min\{v(y), \underbrace{\widehat{v}(x)}_{\geq 0}\},$$

e portanto necessariamente $v(y) \geq 0$, ou seja, $y \in \mathcal{O}_v$. Agora, como $y \in (x + \mathcal{M}_{\widehat{v}})$, temos que a classe de resíduos de y é mapeada pela aplicação acima também em $\overline{x} = x + \mathcal{M}_{\widehat{v}}$, donde é sobrejetiva.

De maneira similar, a aplicação $v(K^\times) \to \widehat{v}(\widehat{K}^\times)$ mandando $v(x)$ em $\widehat{v}(x)$, para todo $x \in K^\times$, é um monomorfismo de grupos, pois

$$x \in K \text{ e } \widehat{v}(x) = 0 \overset{\widehat{v}|_K = v}{\Rightarrow} v(x) = 0.$$

Além disso, preserva a ordem, pois $\widehat{v}|_k = v$.

A fim de mostrar a sobrejetividade, seja $x \in \widehat{K}^\times$. Pela densidade de K em $\widehat{K}$ existe $z \in K$ com

$$\widehat{|z - x|} < \widehat{|x|} = \epsilon,$$

ou seja,

$$\widehat{v}(z - x) > \widehat{v}(x).$$

Mas então

$$\widehat{v}(z) = \widehat{v}(x)$$

pelo Lema 3.2.11.

■

Voltemos aos Exemplos 3.1.6 e 3.1.7 (também tratados nos Exemplos 3.2.3 e 3.2.4) vistos agora na notação aditiva. Nestes exemplos o grupo de valores $v(K^\times)$ é o grupo aditivo $\mathbb{Z}$ dos números inteiros.

Definição 3.2.20 *Se v é um valor absoluto em um corpo K que satisfaz $v(K^\times) = \mathbb{Z}$ então qualquer elemento $\pi \in K$ que satisfaz $v(\pi) = 1$ é chamado um uniformizador de v, ou um parâmetro local. Tal valor absoluto é chamado discreto (de posto 1).*

O uniformizador π tem a seguinte propriedade: todo elemento x de $K^\times$ pode ser escrito como um produto

$$x = u\pi^\nu,$$

onde u é uma unidade de $\mathcal{O}_v$ e $\nu \in \mathbb{Z}$. De fato, se $\nu = v(x)$, então

$$v(x\pi^{-\nu}) = v(x) - \nu v(\pi) = \nu - \nu = 0.$$

Logo $u = x\pi^{-\nu}$ é uma unidade em $\mathcal{O}_v$ satisfazendo $x = u\pi^\nu$. Em particular, o ideal maximal $\mathcal{M}_v$ é principal e gerado por π. É fácil ver que todo ideal de $\mathcal{O}_v$ é principal (gerado por qualquer elemento de valorização mínima dentro do ideal) e é gerado por alguma potência π^n com $n \in \mathbb{N}$. Portanto $\mathcal{O}_v$ é um domínio fatorial.

No caso do Exemplo 3.1.6,

Definição 3.2.21 *O completamento de $(\mathbb{Q}, v_p)$ é chamado corpo dos números p-ádicos e é denotado por $\mathbb{Q}_p$. O anel de valorização de $\mathbb{Q}_p$ é denotado por $\mathbb{Z}_p$, e é chamado o anel dos números p-ádicos.*

O anel $\mathbb{Z}_p$, como veremos abaixo, é o fecho topológico de $\mathbb{Z}$ em $\mathbb{Q}_p$. De acordo com a discussão anterior a este exemplo, o Teorema 3.2.19 e o Exemplo 3.2.3 implicam que o corpo de resíduos de $\mathbb{Z}_p$ é $\mathbb{F}_p$. Observe também que p é um uniformizador para v_p em ambos os corpos, $\mathbb{Q}$ e $\mathbb{Q}_p$.

Os comentários acima são casos especiais do seguinte resultado mais geral:

Proposição 3.2.22 *Sejam v um valor absoluto discreto no corpo K e $\pi \in K$ um uniformizador de v. Então todo elemento $x \in K^\times$ pode ser escrito unicamente como uma série convergente*

$$x = r_\nu \pi^\nu + r_{\nu+1}\pi^{\nu+1} + r_{\nu+2}\pi^{\nu+2} + \ldots = \lim_{n\to\infty} \sum_{i=\nu}^{n} r_i \pi^i,$$

onde $\nu = v(x)$, $r_\nu \neq 0$, e os coeficientes r_i são tomados de um conjunto $R \subseteq \mathcal{O}_v$ de representantes das classes de resíduos no corpo $\overline{K}_v$ (ou seja, a aplicação canônica $\mathcal{O}_v \to \overline{K}_v$ induz uma bijeção de R sobre $\overline{K}_v$).

Prova. Definimos a série por iteração. Como observado acima, $u = x\pi^{-\nu}$ é uma unidade em $\mathcal{O}_v$. Escolha $r_\nu \in R$ tal que $\overline{r_\nu} = \overline{u}$. Então claramente $v(x\pi^{-\nu} - r_\nu) > 0$ ou, equivalentemente,

$$v(x - r_\nu \pi^\nu) > v(\pi^\nu) = \nu.$$

Sejam $x_1 = x - r_\nu \pi^\nu$ e $\mu = v(x_1) > \nu$. Então pelo mesmo argumento temos $r_\mu \in R$ tal que

$$v(x - (r_\nu \pi^\nu + r_\mu \pi^\mu)) = v(x_1 - r_\mu \pi^\mu) > \mu.$$

Repetindo este argumento e adicionando "coeficientes zero" (ou seja representantes para o zero em $\overline{K}_v$) se necessário, obtemos a existência de uma "série"

$$r_\nu \pi^\nu + r_{\nu+1}\pi^{\nu+1} + \ldots$$

Ao mesmo tempo vemos que tal série converge para x, uma vez que

$$v\left(x - \sum_{i=\nu}^{n} r_i \pi^i\right)$$

cresce estritamente, à medida que n cresce.

Mostremos agora a unicidade dos coeficientes: se ${r_\nu}'\pi^\nu + {r_{\nu+1}}'\pi^{\nu+1} + ...$ fosse uma outra representação para x, então 0 teria para representação

$$0 = (r_m - r'_m)\pi^m + (r_{m+1} - r'_{m+1})\pi^{m+1} + ...$$

com $r_m \neq r'_m$ e $r_m, r'_m \in R$, para algum $m \in \mathbb{N}$; considerando m minimal para esta propriedade, teríamos $\overline{r_m - r'_m} \neq \overline{0}$, o que acarretaria $v(0) = m$, uma contradição.

■

Exemplo 3.2.23 *Retornando mais uma vez para o nosso exemplo típico dos números p-ádicos (tratado nos Exemplos 3.1.6 e 3.2.4), temos que, escolhendo para conjunto dos representantes o conjunto*

$$R = \{0, ..., p-1\}$$

e p para uniformizador, qualquer número p-ádico $z \in \mathbb{Q}_p^\times$ tem uma representação única na forma

$$z = \sum_{i=m}^{\infty} a_i p^i,$$

onde $m = v_p(z)$, $0 \leq a_i < p$ para todo i, e $a_m \neq 0$. Se $z \in \mathbb{Z}_p$, ou seja, $v(z) \geq 0$, então

$$z = \sum_{i=0}^{\infty} a_i p^i = \lim_{n\to\infty} \sum_{i=0}^{n} a_i p^i.$$

Isto mostra, em particular, que $\mathbb{Z}$ é denso em $\mathbb{Z}_p$. Mas devemos tomar cuidado ao operarmos com duas tais séries: a adição de duas "séries" da forma $\sum_{i=m}^{\infty} a_i p^i$ não é obtida pela soma coeficiente a coeficiente, porque o conjunto R não necessariamente é fechado pela adição. Escolhendo $p = 7$,

um exemplo simples é

$$5 \times 7^i + 4 \times 7^i = \underbrace{(5+4)}_{\notin R=\{0.1,\ldots,6\}} \times 7^i = (2+7) \times 7^i = 7^{i+1} + 2 \times 7^i.$$

Exemplo 3.2.24 *Para a valorização X-ádica de $k(X)$, podemos tomar para representantes do corpo residual os elementos de k, pois $\overline{K} = k$. Neste caso, todo $z \in k((X))^\times$ tem uma representação única da forma*

$$z = \sum_{i=m}^{\infty} a_i X^i,$$

onde $v_X(z) = m \in \mathbb{Z}$ e $a_i \in k$ para todo i. Desta vez a soma de duas séries coincide com a soma coeficiente a coeficiente. Estas séries são as chamadas séries formais de Laurent. Elas formam um corpo $k((X))$, o corpo das séries formais de Laurent. O valor absoluto discreto canônico sobre $k((X))$ é dado por

$$v\left(\sum_{i=m}^{\infty} a_i X^i\right) = m \text{ se } a_m \neq 0.$$

Claramente o seu anel de valorização consiste do anel $k[[X]]$ das séries de potências formais, ou seja, séries do tipo $\sum_{i=o}^{\infty} a_i X^i$.

3.3 Grupos Abelianos Ordenados e Valorizações

Generalizamos aqui os valores absolutos não-arquimedianos v sobre um corpo K, pinçando as propriedades relevantes do conjunto $v(K^\times)$. Definimos então valorização de Krull. Para tal, começamos com o conceito de grupo abeliano ordenado e apresentamos algumas de suas propriedades.

Definição 3.3.1 *Um grupo abeliano totalmente ordenado é um grupo abeliano (que vamos sempre denotar aditivamente) que admite uma relação de ordem total que é compatível com a operação do grupo. Podemos tornar mais precisa esta definição de duas formas equivalentes: a primeira, falando do grupo abeliano $\langle \Gamma; + \rangle$, com uma relação binária $<$ em Γ que sa-*

tisfaz, para todos $\gamma, \delta, \lambda \in \Gamma$,

$$\left.\begin{array}{ll} (1)\ \gamma \not< \gamma; & (\textit{antissimetria}) \\ (2)\ \gamma < \delta \ e\ \delta < \lambda \ \Rightarrow \gamma < \lambda; & (\textit{transitividade}) \\ (3)\ \gamma < \delta \ \textit{ou}\ \gamma = \delta \ \textit{ou}\ \delta < \gamma; & (\textit{ordem total}) \\ (4)\ \gamma < \delta \ \Rightarrow\ \gamma + \lambda < \delta + \lambda; & (\textit{compatibilidade}) \end{array}\right\} \quad (15)$$

a segunda, falando do grupo abeliano $\langle \Gamma; + \rangle$, *com uma relação binária* $\leq$ *em* Γ *que satisfaz, para todos* $\gamma, \delta, \lambda \in \Gamma$,

$$\left.\begin{array}{ll} (1')\ \gamma \leq \gamma; & (\textit{reflexividade}) \\ (2')\ \gamma \leq \delta\ ,\ \delta \leq \gamma \ \Rightarrow \delta = \gamma; & (\textit{antissimetria})' \\ (3')\ \gamma \leq \delta\ ,\ \delta \leq \lambda \ \Rightarrow \gamma \leq \lambda; & (\textit{transitividade}) \\ (4')\ \gamma \leq \delta \ \textit{ou}\ \delta \leq \gamma; & (\textit{ordem total})' \\ (5')\ \gamma \leq \delta \ \Rightarrow \gamma + \lambda \leq \delta + \lambda; & (\textit{compatibilidade}) \end{array}\right\} \quad (16)$$

A equivalência entre (15) e (16) pode ser facilmente conferida se definimos, a partir da relação $<$, a relação $\leq$ por

$$\gamma \leq \delta \quad \text{se e só se} \quad \gamma < \delta \ \text{ ou } \ \gamma = \delta$$

e, a partir da relação $\leq$, a relação $<$ por

$$\gamma < \delta \quad \text{se e só se} \quad \text{não é verdade que } \delta \leq \gamma.$$

Utilizaremos alternadamente as relações $\leq$ e $<$, e escreveremos simplesmente Γ quando estiver claro a qual relação de ordem nos referimos.

Definição 3.3.2 *Um subgrupo* Δ *de um grupo ordenado* $\langle \Gamma; \leq; +; 0 \rangle$ *é dito convexo em* Γ *se, para cada* $\gamma \in \Gamma$ *e cada* $\delta_1, \delta_2 \in \Delta$, *tem-se*

$$\delta_1 \leq \gamma \leq \delta_2 \Rightarrow \gamma \in \Delta,$$

ou, equivalentemente, para cada $\gamma \in \Gamma$ *e cada* $\delta \in \Delta$,

$$0 \leq \gamma \leq \delta \Rightarrow \gamma \in \Delta.$$

O número de subgrupos convexos próprios de Γ é denominado posto de Γ.

Claramente, a coleção de todos os subgrupos convexos próprios de Γ é linearmente ordenado pela inclusão.

Exemplo 3.3.3 *Se $\{0\}$ é o único subgrupo convexo de Γ, temos que Γ tem posto 1. Isto ocorre, por exemplo, quando $\Gamma = \mathbb{Z}$, justificando a Definição 3.2.20.*

Definição 3.3.4 *Uma ordem $\leq$ em um grupo abeliano Γ é chamada aquimediana se, para todo $\gamma, \epsilon \in \Gamma$,*

$$\epsilon > 0 \Rightarrow \text{existe } n \in \mathbb{N} \text{ tal que } \gamma \leq n\epsilon.$$

Exemplo 3.3.5 *Grupos ordenados arquimedianos só admitem subgrupos convexos triviais. De fato, se Δ é um subgrupo convexo não trivial de Γ e Γ é arquimediano então, dados $\gamma \in \Gamma \backslash \Delta$ e $0 < \delta \in \Delta$, deveria existir $n \in \mathbb{N}$ com $\gamma < n\delta$; por outro lado, pela convexidade de Δ, deveríamos ter $\gamma \in \Delta$, uma contradição. Logo, $\Delta = \{0\}$ e Γ tem posto 1.*

Exemplo 3.3.6 *Todo subgrupo Δ do grupo aditivo $\langle \mathbb{R}; +; 0 \rangle$ dos reais é arquimediano com respeito à ordem canônica $\leq$ induzida por $\mathbb{R}$. Logo, pelo exemplo acima, Δ tem sempre posto 1, exceto para $\Delta = \{0\}$. A recíproca desta observação também é verdadeira, conforme nos mostra a Proposição a seguir.*

Definição 3.3.7 *Um isomorfismo de ordem ou um ordem-isomorfismo entre dois grupos abelianos totalmente ordenados $\langle \Gamma_1, \leq_1 \rangle$ e $\langle \Gamma_2, \leq_2 \rangle$ é um isomorfismo de grupos*

$$\tau : \Gamma_1 \to \Gamma_2$$

que preserva a ordem, isto é, para quaisquer $x, y \in \Gamma_1$,

$$x \leq_1 y \Rightarrow \tau(x) \leq_2 \tau(y).$$

Proposição 3.3.8 *Um grupo abeliano ordenado Γ é de posto 1 se e somente se é ordem-isomorfo a algum subgrupo não-trivial de $\langle \mathbb{R}; +; 0 \rangle$ com a ordem canônica induzida por $\mathbb{R}$.*

Prova. A prova é feita em vários passos.

Fixado $\epsilon > 0$, consideramos o conjunto

$$\Delta_\epsilon = \{\gamma \in \Gamma \mid \gamma, -\gamma \leq n\epsilon, \text{ para algum } n \in \mathbb{N}\}.$$

Afirmação 1: Δ_ϵ é um subgrupo convexo de Γ.

De fato,

- é claro que $0 \in \Delta_\epsilon$ e $-\gamma \in \Delta_\epsilon$ para todo $\gamma \in \Delta_\epsilon$.
- Para $\gamma_1, \gamma_2 \in \Delta_\epsilon$, existem $n_1, n_2 \in \mathbb{N}$ com

$$\gamma_1, -\gamma_1 < n_1\epsilon \quad \text{e} \quad \gamma_2, -\gamma_2 < n_2\epsilon,$$

e disto segue que

$$(\gamma_1 + \gamma_2), -(\gamma_1 + \gamma_2) < (n_1 + n_2)\epsilon.$$

Logo, Δ_ϵ é um subgrupo de Γ.

- Claramente Δ_ϵ é convexo, ou seja, se $\gamma \in \Gamma$, $\delta \in \Delta_\epsilon$, digamos,

$$\delta, -\delta \leq n\epsilon,$$

com $\epsilon > 0$, e se $0 \leq \gamma \leq \delta$ então $\gamma, -\gamma \leq n\epsilon$, o que implica $\gamma \in \Delta_\epsilon$.

Afirmação 2 : Todo grupo Γ de posto 1 é arquimediano.

De fato, fixado $\epsilon \in \Gamma$ com $\epsilon > 0$, basta provar que para todo $\gamma \in \Gamma$ existe algum $n \in \mathbb{N}$ tal que $\gamma, -\gamma \leq n\epsilon$.

Daí, como $0 \neq \epsilon \in \Delta_\epsilon$, temos $\Delta_\epsilon \neq \{0\}$; como Γ tem por hipótese posto 1, concluímos que $\Delta_\epsilon = \Gamma$, o que completa a prova da Afirmação 2.

Para o resto da prova, fixamos um elemento positivo $\epsilon \in \Gamma$, e para cada $\alpha \in \Gamma$ definimos

$$L(\alpha) = \{m/n \in \mathbb{Q} \mid n > 0 \text{ e } m\epsilon \leq n\alpha\}$$

$$\text{e} \quad U(\alpha) = \{m/n \in \mathbb{Q} \mid n > 0 \text{ e } n\alpha \leq m\epsilon\}.$$

Afirmação 3: Para cada $\alpha \in \Gamma$, $L(\alpha)$ e $U(\alpha)$ definem um corte de Dedekind em $\mathbb{Q}$, ou seja.

- $L(\alpha) \neq \emptyset \neq U(\alpha)$;
- $L(\alpha) \cup U(\alpha) = \mathbb{Q}$;
- se $\beta \in L(\alpha)$ e $\beta' \in U(\alpha)$ então $\beta \leq \beta'$,

De fato,

- como Γ é ordenado, para cada racional m/n com $n > 0$ temos, por (4') de (16),

$$m\epsilon \leq n\alpha \quad \text{ou} \quad m\epsilon \geq n\alpha,$$

e assim todo racional está em $L(\alpha)$ ou em $U(\alpha)$. Logo $L(\alpha) \cup U(\alpha) = \mathbb{Q}$.

- Se $L(\alpha) = \emptyset$, então $\mathbb{Q} = L(\alpha) \cup U(\alpha) = U(\alpha)$, e com isto, em particular, $m\epsilon \leq \alpha$ para todo $m \in \mathbb{Z}$, o que é impossível já que Γ é arquimediano. Por um raciocínio similar conclui-se que $U(\alpha) \neq \emptyset$.

- Para confirmar a última propriedade, se $\beta = a/b \in L(\alpha)$ e $\beta' = c/d \in U(\alpha)$ então

$$a\epsilon \leq b\alpha \quad \text{e} \quad d\alpha \leq c\epsilon;$$

daí, como $b > 0$ e $d > 0$,

$$ad\epsilon \leq bd\alpha \quad \text{e} \quad bd\alpha \leq bc\epsilon,$$

e portanto

$$ad\epsilon \leq bc\epsilon;$$

como $\epsilon > 0$, concluímos:

$$ad \leq bc, \quad \text{isto é,} \quad \beta = \frac{a}{b} \leq \frac{c}{d} = \beta'.$$

Assim, existe uma aplicação $\alpha \mapsto r(\alpha)$ do grupo ordenado Γ no grupo aditivo $\langle \mathbb{R}; + \rangle$ onde $r(\alpha)$ é o número real correspondente ao corte de Dedekind definido por $L(\alpha)$ e $U(\alpha)$, mais precisamente:

$$r(\alpha) = \sup(L(\alpha)) = \inf(U(\alpha)).$$

Claramente $\alpha \leq \beta$ implica $r(\alpha) \leq r(\beta)$.

Afirmação 4: r é um monomorfismo de grupos.

De fato, para $\alpha, \beta \in \Gamma$ sejam $m/n \in L(\alpha)$ e $m'/n' \in L(\beta)$. Sem perda de generalidade, podemos supor $n' = n$. Daí,

$$m\epsilon \leq n\alpha \quad \text{e} \quad m'\epsilon \leq n\beta \Rightarrow (m+m')\epsilon \leq n(\alpha+\beta) \Rightarrow (m+m')/n \in L(\alpha+\beta).$$

Logo

$$L(\alpha) + L(\beta) \subseteq L(\alpha + \beta).$$

Disto segue

$$r(\alpha) + r(\beta) \leq r(\alpha + \beta).$$

De maneira similar prova-se que

$$U(\alpha) + U(\beta) \subseteq U(\alpha + \beta).$$

Como a última inclusão implica

$$r(\alpha + \beta) \leq r(\alpha) + r(\beta),$$

conclúmos

$$r(\alpha) + r(\beta) = r(\alpha + \beta),$$

e portanto r é um homomorfismo de grupos.

Finalmente,

$$r(\alpha) = 0 \Rightarrow$$
$$-1/n \in L(\alpha) \text{ e } 1/n \in U(\alpha),$$

para todo inteiro positivo n. Portanto,

$$-\epsilon \leq n\alpha \leq \epsilon$$

para todo $n > 0$. Como o grupo Γ é arquimediano, concluímos que $\alpha = 0$.

■

Sejam Γ um grupo abeliano ordenado e $\Delta \subseteq \Gamma$ um subgrupo convexo. Então o grupo quociente Γ/Δ pode ser visto como um grupo ordenado também:

Proposição 3.3.9 *Sejam Γ um grupo abeliano ordenado e $\Delta \subseteq \Gamma$ um subgrupo convexo. Então, se $\gamma + \Delta$ e $\gamma' + \Delta$ são classes laterais distintas, podemos ordená-las definindo*

$$\gamma + \Delta < \gamma' + \Delta \quad se \quad \gamma + h_1 < \gamma' + h_2 \tag{17}$$

para todo $h_1, h_2 \in \Delta$.

Prova. Ressaltamos inicialmente que esta definição independe dos representantes, pois se $\gamma + \Delta = \gamma_1 + \Delta$ e $\gamma' + \Delta = \gamma_1' + \Delta$ temos

$$\gamma = \gamma_1 + h_* \quad \text{e} \quad \gamma' = \gamma_1' + h_*',$$

para certos $h_*, h_*' \in \Delta$. Se tivermos $\gamma + \Delta < \gamma' + \Delta$, então, pela definição, temos que

$$\gamma_1 + h = \gamma + (h - h_*) \overset{\gamma+\Delta<\gamma'+\Delta}{<} \gamma' + (h' - h_*') = \gamma_1' + h',$$

para todo $h, h' \in \Delta$, ou seja,

$$\gamma_1 + \Delta < \gamma_1' + \Delta.$$

De $\gamma \not< \gamma$ segue por exemplo que $\gamma + \Delta \not< \gamma + \Delta$. A transitividade e a compatibilidade também são claras. Para assegurar que a ordem é total precisamos da propriedade de Δ ser convexo. De fato, suponhamos que $\gamma+\Delta \not< \gamma'+\Delta$ e que $\gamma'+\Delta \not< \gamma+\Delta$. Neste caso, existem $h_1, h_2, h_3, h_4 \in \Delta$ com

$$\gamma + h_1 \leq \gamma' + h_2 \quad \text{e} \quad \gamma' + h_3 \leq \gamma + h_4$$

ou seja

$$\gamma - \gamma' \leq h_2 - h_1 \in \Delta \quad \text{e} \quad -(\gamma - \gamma') \leq h_4 - h_3 \in \Delta$$

e portanto

$$h_3 - h_4 \leq \gamma - \gamma' \leq h_2 - h_1 \in \Delta$$

Como Δ é convexo concluímos que $(\gamma - \gamma') \in \Delta$. Mas isto implica que $\gamma + \Delta = \gamma' + \Delta$.

Com isto, provamos que a relação $<$ em Γ/Δ é uma relação de ordem total.

■

Desta definição e da convexidade de Δ podemos mostrar também a seguinte equivalência: se $\gamma + \Delta$ e $\gamma' + \Delta$ são classes distintas então

$$\gamma + \Delta < \gamma' + \Delta \quad \text{se e só se} \quad \gamma < \gamma'. \tag{18}$$

Obviamente a implicação da esquerda para a direita é trivial. Falta mostrar a implicação na direção contrária. De fato, caso contrário existiriam $h_1, h_2 \in \Delta$ com

$$\gamma + h_1 \geq \gamma' + h_2 \Rightarrow \underbrace{h_1 - h_2}_{\in \Delta} \geq \gamma' - \gamma > 0$$

$$\overset{\Delta \text{ é convexo}}{\Rightarrow} \gamma' - \gamma \Rightarrow \gamma' + \Delta = \gamma + \Delta,$$

absurdo.

Exemplo 3.3.10 *Salientamos que sem a hipótese de Δ ser convexo não*

poderíamos garantir que a relação definida em (17) torna o grupo quociente totalmente ordenado. De fato, considerando $\Gamma = \mathbb{Z}$ *com a ordem usual e* $\Delta = 2\mathbb{Z}$*, que obviamente não é convexo, afirmamos que*

$$1 + 2\mathbb{Z} \neq 0 + 2\mathbb{Z} \quad , \quad 1 + 2\mathbb{Z} \not< 0 + 2\mathbb{Z} \quad e \quad 0 + 2\mathbb{Z} \not< 1 + 2\mathbb{Z}.$$

De fato, é claro que as classes são distintas; além disso, de

$$\underbrace{0+0}_{\in 0+2\mathbb{Z}} \; < \; \underbrace{1+0}_{\in 1+2\mathbb{Z}},$$

concluímos que $1 + 2\mathbb{Z} \not< 0 + 2\mathbb{Z}$*; e, de*

$$\underbrace{1+0}_{\in 1+2\mathbb{Z}} \; < \; \underbrace{0+2}_{\in 0+2\mathbb{Z}},$$

concluímos que $0 + 2\mathbb{Z} \not< 1 + 2\mathbb{Z}$*.*

Exemplo 3.3.11 *Generalizando: se* Γ *é um grupo abeliano ordenado e* Δ *é um subgrupo que não é convexo, então existem* $\delta \in \Delta$ *e* $\gamma \in \Gamma \backslash \Delta$ *com* $0 < \gamma < \delta$*. Com isto, pela definição da relação* $<$ *(veja (17)), teríamos que*

$$\gamma \notin \Delta \Rightarrow \gamma + \Delta \neq \delta + \Delta$$

$$\gamma < \delta. \Rightarrow \gamma + 0 < \delta + 0 \Rightarrow \delta + \Delta \not< \gamma + \Delta$$

$$0 < \gamma \Rightarrow \delta + 0 < \gamma + \delta \Rightarrow \gamma + \Delta \not< \delta + \Delta.$$

Assim, concluímos que $<$ *não satisfaz a propriedade (3) de (15).*

Definição 3.3.12 *Se* Γ *e* Δ *são dois grupos abelianos ordenados, podemos ordenar lexicograficamente o produto direto* $\Gamma \times \Delta$*, tomando, para cada* $\gamma, \gamma' \in \Gamma$ *e* $\delta, \delta' \in \Delta$*,*

$$(\gamma, \delta) \leq (\gamma', \delta') \quad \text{se e só se} \quad \gamma < \gamma' \text{ ou } (\gamma = \gamma' \text{ e } \delta \leq \delta'),$$

onde $\leq$ *é definida a partir de* $<$ *da seguinte forma:*

$$\gamma + \Delta \leq \gamma' + \Delta \quad \text{se e só se} \quad \gamma + \Delta = \gamma' + \Delta \text{ ou } (\gamma = \gamma' \text{ e } \delta \leq \delta').$$

Claramente $\{0\} \times \Delta$ torna-se um subgrupo convexo de $\Gamma \times \Delta$, ordem isomorfo a Δ.

Exemplo 3.3.13 *O produto lexicográfico $\mathbb{Z} \times \mathbb{Z}$ é de posto 2, e, no caso mais geral $\mathbb{Z}^n = \mathbb{Z} \times ... \times \mathbb{Z}$ quando também ordenado lexicograficamente, é de posto n.*

Observação 3.3.14 *No entanto, podemos dar para $\mathbb{Z}\times\mathbb{Z}$ uma outra ordem que faz dele um grupo abeliano ordenado de posto 1. De fato, podemos identificar $\mathbb{Z} \times \mathbb{Z}$ com o subgrupo $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ do grupo aditivo dos reais e tomar a ordem induzida por $\mathbb{R}$.*

Definição 3.3.15 *Um grupo abeliano ordenado que admite um elemento positivo minimal é dito discreto, caso contrário é dito densamente ordenado ou simplesmente denso.*

Exemplo 3.3.16 *Com respeito à ordem lexicográfica, $\mathbb{Z} \times \mathbb{Z}$ é um grupo discreto de posto 2; com respeito à ordem induzida por $\mathbb{R}$, $\mathbb{Z} \times \mathbb{Z}$ não é discreto, e por isso é denso.*

Observação 3.3.17 *Todo grupo abeliano ordenado Γ é livre de torção, ou seja, para $n \in \mathbb{N}\backslash\{0\}$ e $\gamma \in \Gamma$*

$$n\gamma = 0 \;\Rightarrow\; \gamma = 0.$$

De fato, para $\Gamma = \{0\}$ a afirmação é trivial. E, se existe $\gamma \in \Gamma$ com $\gamma \neq 0$, então $\gamma < 0$ ou $\gamma > 0$. Assim, usando a compatibilidade em (15), temos, para todo $n \in \mathbb{N}\backslash\{0\}$,

$$0 < \gamma < \gamma + \gamma < ... < n\gamma \quad ou \quad 0 > \gamma > \gamma + \gamma > ... > n\gamma,$$

e portanto, em qualquer caso, $n\gamma \neq 0$.

Depois desta curta incursão por grupos abelianos ordenados, definimos valorização de Krull:

Definição 3.3.18 *Sejam Γ um grupo abeliano ordenado, e ∞ um símbolo satisfazendo as regras:*

$$\infty = \infty + \infty = \gamma + \infty = \infty + \gamma, \text{ para todo } \gamma \in \Gamma. \tag{19}$$

Uma valorização (de Krull) v sobre um corpo K é uma aplicação sobrejetiva

$$v : K \twoheadrightarrow \Gamma \cup \{\infty\},$$

satisfazendo os seguintes axiomas para todo $x, y \in K$:

1. $v(x) = \infty \Leftrightarrow x = 0$,
2. $v(xy) = v(x) + v(y)$,
3. $v(x + y) \geq \min\{v(x), v(y)\}$.

O grupo $\Gamma = v(K^\times)$ é chamado o grupo de valores de v.

Claramente esta definição generaliza a Definição 3.2.1, com a diferença que a sobrejetividade não era lá requerida. Aqui ela está sendo requerida apenas para facilitar a notação e o uso do grupo de valores.

Definição 3.3.19 *Se $v(K^\times) = \{0\}$ chamamos v de valorização trivial. O posto de v é o posto do grupo de valores $v(K^\times)$.*

Listamos agora algumas propriedades que continuam sendo satisfeitas pelas valorizações de Krull.

Lema 3.3.20 *Seja $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ uma valorização. Então*

(*i*) $v(1) = 0$.

E, para todos $x, y \in K^\times$,

(*ii*) $v(x^{-1}) = -v(x)$.

(*iii*) $v(-x) = v(x)$.

(*iv*) $v(x) < v(y) \Rightarrow v(x+y) = v(x)$. *Em geral:*

$$v(x_1) < v(x_i), \text{ para todo } i \in \{2, ..., n\} \Rightarrow v(x_1 + ... + x_n) = v(x_1).$$

Prova. Da Definição 3.3.18 obtemos:

(*i*) $v(1) = 0$, pois

$$v(1) = v(1.1) = v(1) + v(1).$$

(*ii*) $v(x^{-1}) = -v(x)$, pois

$$0 = v(1) = v(x.x^{-1}) = v(x) + v(x^{-1}).$$

(*iii*) Inicialmente observemos que

$$v(-1) = v((-1)^{-1}) = -v(-1),$$

donde

$$v(-1) = 0.$$

Então

$$v(-x) = v((-1).x) = v(-1) + v(x) = v(x).$$

(*iv*) A prova aqui é idêntica às provas do Lema 3.2.11 e Corolário 3.2.12.

■

Dada uma valorização $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$, é fácil ver que o conjunto

$$\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$$

é um anel de valorização de K, isto é, um subanel de K tal que para todo $x \in K^\times$,

$$x \in \mathcal{O}_v \text{ ou } x^{-1} \in \mathcal{O}_v.$$

e portanto o grupo multiplicativo $\mathcal{O}_v^\times$ das unidades de $\mathcal{O}_v$ é dado por

$$\mathcal{O}_v^\times = \{x \in K \mid v(x) = 0\}.$$

O conjunto das não-unidades

$$\mathcal{M}_v = \{x \in K \mid v(x) > 0\}$$

forma um ideal maximal de $\mathcal{O}_v$, de fato o único ideal maximal pois qualquer outro deveria então conter uma unidade.

Resumimos abaixo estes fatos e fazemos uma definição.

Definição 3.3.21 *Dada uma valorização v, o anel de valorização de v e o ideal maximal de v são, nesta ordem, os conjuntos*

$$\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\} \quad e \quad \mathcal{M}_v = \{x \in K \mid v(x) > 0\}.$$

O quociente

$$\overline{K_v} := \mathcal{O}_v/\mathcal{M}_v$$

é chamado o corpo de resíduos de v.

Agora mostramos que, reciprocamente, todo anel de valorização $\mathcal{O}$ de K determina uma valorização sobre K.

Proposição 3.3.22 *Seja $\mathcal{O} \subset K$ um anel de valorização de K. Então existe uma valorização v sobre K tal que $\mathcal{O} = \mathcal{O}_v$.*

Prova. Denotamos por $\mathcal{O}^\times$ o grupo multiplicativo das unidades de $\mathcal{O}$. O grupo quociente (multiplicativo) $\Gamma = K^\times/\mathcal{O}^\times$ é um grupo abeliano. Nós o reescrevemos aditivamente definindo para as classes $x\mathcal{O}^\times$ e $y\mathcal{O}^\times$:

$$x\mathcal{O}^\times + y\mathcal{O}^\times := xy\mathcal{O}^\times.$$

Definimos uma ordem por

$$x\mathcal{O}^\times \leq y\mathcal{O}^\times \Leftrightarrow \frac{y}{x} \in \mathcal{O}.$$

É fácil convencer-se que, desta forma, Γ se torna um grupo abeliano ordenado. A única propriedade que não é provada usando apenas a definição

de anel e de ordem é a propriedade (4') de (16): para todo $\gamma, \delta \in \Gamma$,

$$\gamma \leq \delta \quad \text{ou} \quad \delta \leq \gamma,$$

que segue da propriedade de que em um anel de valorização x ou $x^{-1} \in \mathcal{O}$. Definimos então

$$v(x) := \begin{cases} x\mathcal{O}^\times \in \Gamma = K^\times/\mathcal{O}^\times, \text{ para } x \in K^\times \\ \infty, \text{ para } x = 0. \end{cases}$$

Afirmamos que v é a desejada valorização. De fato,

· $v(x.y) = v(x) + v(y)$ é trivial.

· Se $v(x) \leq v(y)$, então $y/x \in \mathcal{O}$ e portanto também

$$(x+y)/x = 1 + y/x \in \mathcal{O}.$$

Logo

$$v(x+y) \geq v(x) = \min\{v(x), v(y)\}.$$

· Obviamente,

$$\mathcal{O}_v = \{x \in K \mid v(x) \geq 0 = v(1)\} = \left\{x \in K \mid \frac{x}{1} \in \mathcal{O}\right\} = \mathcal{O}.$$

■

A proposição acima implica que o conjunto $\mathcal{M} = \mathcal{O}\backslash\mathcal{O}^\times$ é um ideal do anel de valorização $\mathcal{O}$. Mais precisamente, por esta caracterização, o seu único ideal maximal. Estendemos o conceito de posto de valorização para anéis de valorização:

Definição 3.3.23 *O posto de um anel de valorização $\mathcal{O}$ é o posto do seu grupo de valores da valorização a ele associada, ou seja, $\Gamma = K^\times/\mathcal{O}^\times$.*

Exemplo 3.3.24 *O anel de valorização $\mathcal{O} = K$ claramente corresponde à valorização trivial, e será chamado anel de valorização trivial. Num corpo finito o único anel de valorização é o trivial pois, por um lado, a valorização correspondente tem para grupo de valores $K^\times/\mathcal{O}^\times$ que então*

é obviamente finito; mas por outro lado, por ser um grupo ordenado, se existir um elemento α maior que 0 então tal grupo deveria possuir uma infinidade de elementos:

$$0 < \alpha < \alpha + \alpha < ...,$$

uma contradição.

Definição 3.3.25 *Duas valorizações de um corpo K,*

$$v_i : K \twoheadrightarrow \Gamma_i \cup \{\infty\},$$

para $i \in \{1, 2\}$, são ditas equivalentes se definem o mesmo anel de valorização em K, ou seja,

$$\mathcal{O}_{v_1} = \mathcal{O}_{v_2}.$$

Proposição 3.3.26 *Duas valorizações $v_i : K \twoheadrightarrow \Gamma_i \cup \{\infty\}$ de K são equivalentes se e só se existe um isomorfismo*

$$\rho : \Gamma_1 \to \Gamma_2$$

que preserva a ordem satisfazendo

$$\rho \circ v_1 = v_2.$$

Ou seja, o seguinte diagrama é comutativo:

$$\begin{array}{ccc} K^{\times} & \xrightarrow{v_1} & \Gamma_1 \\ {\scriptstyle v_2}\downarrow & \swarrow{\scriptstyle \rho} & \\ \Gamma_2 & & \end{array}$$

Prova. Se tal $\rho : \Gamma_1 \to \Gamma_2$ existe , então $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$, pois

$$\begin{aligned}\mathcal{O}_{v_2} &= \{x \in K \mid v_2(x) \geq 0\} \\ &= \{x \in K \mid (\rho \circ v_1)(x) \geq 0\} \\ &= \{x \in K \mid \rho(v_1(x)) \geq 0\} \\ &= \{x \in K \mid v_1(x) \geq 0\} = \mathcal{O}_{v_1}.\end{aligned}$$

Reciprocamente, como $v_i : K^\times \twoheadrightarrow \Gamma_i$ é um homomorfismo sobrejetor de grupos ordenados tendo núcleo $\mathcal{O}_{v_i}^\times$ para $i \in \{1, 2\}$, existem isomorfismos

$$\tau_i : K^\times / \mathcal{O}_{v_i}^\times \twoheadrightarrow \Gamma_i$$

satisfazendo

$$\tau_i(x\mathcal{O}_{v_i}^\times) = v_i(x),$$

para $i \in \{1, 2\}$. Salientamos que cada τ_i preserva a ordem. De fato:

$$x\mathcal{O}_{v_i}^\times \geq 1\mathcal{O}_{v_i}^\times \Leftrightarrow x \in \mathcal{O}_{v_i} \Leftrightarrow v_i(x) \geq 0.$$

Como por hipótese $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$ temos

$$K^\times / \mathcal{O}_{v_1}^\times = K^\times / \mathcal{O}_{v_2}^\times.$$

Logo $\rho = \tau_2 \circ \tau_1^{-1}$ é o ordem-isomorfismo desejado.

■

Usando a Proposição 3.3.26, podemos dizer que existe uma correspondência biunívoca entre os anéis de valorização de K e as valorizações de K, a menos de ordem-isomorfismos entre os grupos de valores. Neste sentido, identificamos as valorizações com os anéis de valorização a partir daqui. Usaremos, em cada momento, o que for mais conveniente.

O próximo teorema determina todas as valorizações de $\mathbb{Q}$ e de $k(X)$ que se anulam sobre k.

Definição 3.3.27 *A valorização do grau é simbolizada por v_∞ e definida*

em $k(X)$ *como*

$$v_\infty(0) = 0 \quad e \quad v_\infty\left(\frac{f}{g}\right) = \deg(g) - \deg(f),$$

onde $f, g \in k(X)^\times$.

Teorema 3.3.28

(a) *Toda valorização não trivial de* $\mathbb{Q}$ *é a valorização p-ádica para algum número primo* p.

(b) *Toda valorização não trivial de* $k(X)$ *que se anula sobre* k, *ou é a valorização do grau* v_∞ *ou é uma valorização p-ádica para algum polinômio irredutível* $p \in k[X]$.

Prova. Sejam $K \in \{\mathbb{Q}\ ,\ k(X)\}$ e v uma valorização não trivial sobre K, sendo no segundo caso v suposto trivial sobre k. Isto significa, no segundo caso, que $k \subseteq \mathcal{O}$. Então o anel de valorização $\mathcal{O} = \mathcal{O}_v$ é diferente de K.

(a) Como $1 \in \mathcal{O}$, temos $\mathbb{Z} \subseteq \mathcal{O}$. Como $\mathcal{O} \neq \mathbb{Q}$, segue que pelo menos um primo p deve estar em $\mathcal{M}$:

$$v(p) > 0.$$

Se q é um primo diferente de p temos

$$ap + bq = 1,$$

para certos $a, b \in \mathbb{Z}$. Isto mostra que $q \notin \mathcal{M}$. Portanto todos os primos $q \neq p$ são unidades em $\mathcal{O}$. Usando a fatoração de inteiros vemos portanto que para $a, b \in \mathbb{Z}$ relativamente primos temos

$$\frac{a}{b} \in \mathcal{O} \text{ se e só se } p \nmid b.$$

Isto prova que

$$\mathcal{O} = \mathbb{Z}_{(p)},$$

ou seja, v é equivalente à valorização p-ádica v_p (veja Exemplo 3.2.9).

(b) Aqui temos dois casos a considerar:

- se $X \in \mathcal{O}$ então $k[X] \subseteq \mathcal{O}$ e podemos argumentar como no caso (a) trocando $\mathbb{Z}$ por $k[X]$, concluindo que v é equivalente à valorização p-ádica v_p (veja Exemplo 3.1.7).

- Se $X \notin \mathcal{O}$ então $X^{-1} \in \mathcal{M}$, $v(X) < 0$ e

$$v(X^m) < v(X^n)$$

sempre que $0 \leq n < m$. Como $v(a) = 0$ para todo $a \in k^\times$,

$$v(a_n X^n + a_{n-1} X^{n-1} + ... + a_0) = v(a_n X^n) = nv(X),$$

sempre que $a_n \neq 0$. Portanto, o grupo de valores $v(k(X)^\times)$ é idêntico a $\mathbb{Z}v(X)$. Mandando $v(X)$ em -1 achamos um isomorfismo ρ entre $\mathbb{Z}v(X)$ e $\mathbb{Z}$ que preserva a ordem, o que mostra que v é equivalente à valorização do grau, uma vez que

$$\begin{aligned}(\rho \circ v)(a_n X^n + a_{n-1} X^{n-1} + ... + a_0) &= \rho(nv(X)) \\ &= n\rho(v(X)) = -n \\ &= v_\infty(a_n X^n + a_{n-1} X^{n-1} + ... + a_0).\end{aligned}$$

■

A demonstração acima nos mostra também que a valorização do grau funciona como uma "ordem do pólo zero" no infinito como a vista na teoria de funções meromorfas.

3.4 Anéis de valorização em um corpo

Nesta seção colecionamos vários resultados relativos a valorizações, anéis de valorização e grupos de valores de um corpo fixado; às vezes mostramos relações que existem entre eles. A próxima seção será dedicada à teoria de valorizações relacionada com extensões de corpos.

Começamos ressaltando o que ocorre de especial quando temos um corpo algebricamente fechado. Para tal, precisamos da noção de grupo divisível e algumas de suas propriedades.

Também nos preocupamos com a existência de anéis de valorização em um corpo arbitrário, o que é garantido pelo Teorema de Chevalley. A partir dele conseguimos também caracterizar o fecho inteiro de um domínio D como a interseção dos anéis de valorização que contêm D.

Demonstramos alguns resultados que relacionam valorizações com certas localizações e estabelecemos um resultado que nos leva a uma certa noção de proximidade entre elementos de um corpo com relação a valorizações.

Incluímos ainda alguns resultados que são também necessários quando tratamos de extensões de corpos valorizados.

Definição 3.4.1 *Um grupo abeliano $\langle G\ ;+\rangle$ é dito um grupo divisível quando, para quaisquer $g \in G$ e $n \in \mathbb{N}^*$ existe $h \in G$ tal que*

$$nh = g$$

Exemplo 3.4.2 *$\langle \mathbb{Z}\ ;+\rangle$ não é divisível, mas $\langle \mathbb{Q}\ ;+\rangle$ o é.*

Lema 3.4.3 *O quociente de um grupo divisível por qualquer um de seus subgrupos é também um grupo divisível*

Prova. Sejam G um grupo divisível e H um subgrupo de G. Então, dados $g \in G$, $n \in \mathbb{N}$ e $g' \in G$ tais que

$$ng' = g,$$

temos

$$n\overline{g'} = \overline{g},$$

o que completa a prova.

■

Lema 3.4.4 *Seja L um corpo valorizado algebricamente fechado com valorização v associada. Então*

i) o grupo de valores $v(L^*)$ é um grupo divisível.

ii) o corpo de resíduos $\overline{L}$ é também algebricamente fechado.

Prova. *i)* Dados $a \in L^*$ e $n \in \mathbb{N}^*$, temos que o polinômio

$$X^n - a$$

admite uma raiz em L, que vamos denotar por b. Daí,

$$v(a) = v(b^n) = nv(b),$$

o que prova que $v(L^*)$ é um grupo divisível.

ii) Seja $\overline{f} \in \overline{L}[X]$ um polinômio não constante. Como queremos mostrar que todo polinômio não constante de $L[X]$ admite uma raiz em $\overline{L}$, basta provar este fato para polinômios mônicos.

Dado

$$\overline{a_0} + \overline{a_1}X + ... + X^n \in \overline{L}[X],$$

consideramos

$$f(X) = a_0 + a_1X + ... + X^n \in \mathcal{O}[X] \subset L[X], \tag{20}$$

sendo $\mathcal{O}$ o anel de valorização associado a v. Como L é algebricamente fechado, temos

$$f(X) = \prod_{i=1}^{n}(X - b_i), \quad b_i \in L$$

Afirmamos que para todo i, $b_i \in \mathcal{O}$. De fato,

$$\infty = v(f(b_i)) \overset{(20)}{\geq} \min_{0 \leq j \leq n-1}\{v(a_j) + jb_j), nv(b)\}$$

de modo que se fosse $v(b_i) < 0$, então teríamos

$$\infty = v(f(b_i)) = nv(b_i) < 0,$$

absurdo. Assim, todas as raízes de f em L dão origem a raízes de $\overline{f}$ em $\overline{L}$, de modo que todo polinômio não constante de $\overline{L}[X]$ admite pelo menos

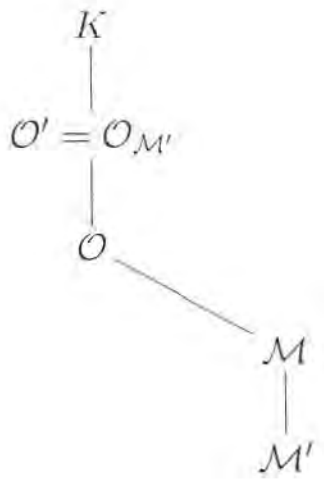
uma raiz.

■

Proposição 3.4.5 *Sejam $\mathcal{O}$ um anel de valorização não trivial de K e $\mathcal{O}' \subseteq K$ um sobreanel de $\mathcal{O}$ (e portanto um anel de valorização de K). Então, denotando por $\mathcal{M}$ e $\mathcal{M}'$ os ideias maximais de $\mathcal{O}$ e $\mathcal{O}'$, respectivamente. Temos:*

(i) $\mathcal{M}' \subseteq \mathcal{M}$

(ii) $\mathcal{O}' = \mathcal{O}_{\mathcal{M}'}$



Prova. (i) De fato,

$$x \in \mathcal{M}' \Rightarrow x^{-1} \notin \mathcal{O}' \overset{\mathcal{O}\subseteq\mathcal{O}'}{\Rightarrow} x^{-1} \notin \mathcal{O} \Rightarrow x \in \mathcal{M}.$$

(ii) Como $\mathcal{M}'$ é um ideal primo de $\mathcal{O}'$ e como $\mathcal{M}' \subseteq \mathcal{M}$, temos que $\mathcal{M}'$ também é um ideal primo de $\mathcal{O}$. Para mostrarmos que $\mathcal{O}' = \mathcal{O}_{\mathcal{M}'}$, começamos verificando que todo elemento de $\mathcal{O}'$ tem a forma a/b com $a, b \in \mathcal{O}$ e $b \notin \mathcal{M}'$. E, de fato, dado $x \in \mathcal{O}'$,

- se $x \in \mathcal{O}$ escrevemos simplesmente

$$x = x/1 \in \mathcal{O}_{\mathcal{M}'};$$

- se $x \notin \mathcal{O}$ temos $x^{-1} \in \mathcal{O} \subseteq \mathcal{O}'$, e portanto $x^{-1} \in \mathcal{M} \backslash \mathcal{M}'$, e neste caso

escrevemos

$$x = 1/x^{-1} \in \mathcal{O}_{\mathcal{M}'}.$$

Agora, dado $s \in \mathcal{O} \backslash \mathcal{M}'$, ou $s \in (\mathcal{O}')^{\times}$ ou $s \notin \mathcal{O}'$, mas em todo caso $s^{-1} \in \mathcal{O}'$. Como $\mathcal{O} \subseteq \mathcal{O}'$, concluímos que $\mathcal{O}_{\mathcal{M}'} \subseteq \mathcal{O}'$ e a igualdade está provada.

■

Observação 3.4.6 *Salientamos que, como na prova acima não excluímos o caso $\mathcal{O}' = K$, o argumento mostra que $K = \mathcal{O}_{\{0\}}$, ou seja, K é o corpo de frações de qualquer anel de valorização $\mathcal{O}$ de K.*

Corolário 3.4.7 *Dado um anel de valorização $\mathcal{O}$ de K, os sobreanéis $\mathcal{O}'$ de $\mathcal{O}$ em K estão em correspondência 1-1 com os ideais primos $\mathfrak{p}$ de $\mathcal{O}$. Esta correspondência reverte a inclusão.*

Prova. A seguinte aplicação nos dá a correspondência

$$\varphi : \{\mathcal{O}' \mid \mathcal{O}' \text{ é sobreanel de } \mathcal{O}\} \to \{\mathfrak{p} \mid \mathfrak{p} \text{ é ideal primo de } \mathcal{O}\}, \quad \varphi(\mathcal{O}') = \mathcal{M}',$$

onde $\mathcal{M}'$ denota o ideal maximal de $\mathcal{O}'$. Ela está bem definida pelo item (i) do resultado anterior.

De fato, esta aplicação possui uma inversa dada por

$$\psi : \{\mathfrak{p} \mid \mathfrak{p} \text{ é ideal primo de } \mathcal{O}\} \to \{\mathcal{O}' \mid \mathcal{O}' \text{ é sobreanel de } \mathcal{O}\}, \quad \psi(\mathfrak{p}) = \mathcal{O}_{\mathfrak{p}}$$

De fato, claramente a localização $\mathcal{O}_{\mathfrak{p}}$ é um sobre-anel de $\mathcal{O}$ com ideal maximal $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. E também é claro que

$$\varphi(\psi(\mathfrak{p})) = \varphi(\mathcal{O}_{\mathfrak{p}}) = \mathfrak{p}\mathcal{O}_{\mathfrak{p}} \overset{\text{Prop.3.4.5}(i)}{=} \mathfrak{p}\mathcal{O}_{\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p}$$

e

$$\psi(\varphi(\mathcal{O}')) = \psi(\mathcal{M}') = \mathcal{O}_{\mathcal{M}'} \overset{\text{Prop.3.4.5}(ii)}{=} \mathcal{O}'.$$

Para mostrar que tal correspondência reverte a inclusão, observamos que,

$$\mathcal{O}' \subseteq \mathcal{O}'' \overset{\text{Prop.3.4.5}(i)}{\Rightarrow} \mathcal{M}'' \subseteq \mathcal{M}' \Rightarrow \varphi(\mathcal{M}'') \subseteq \varphi(\mathcal{M}')$$

■

Agora provamos outra correspondência biunívoca.

Proposição 3.4.8 *Sejam*

$$v : K \twoheadrightarrow \Gamma \cup \{\infty\}$$

uma valorização não trivial de K *e* $\mathcal{O} = \mathcal{O}_v$. *Então existe uma correspondência* $1-1$ *entre os subgrupos convexos* Δ *de* Γ *e os ideais primos de* $\mathcal{O}$. *Esta correspondência é dada por*

$$\Delta \mapsto \mathfrak{p}_\Delta = \{x \in K \mid v(x) > \delta \ , \ \forall \delta \in \Delta\}.$$

$$\mathfrak{p} \mapsto \Delta_\mathfrak{p} = \{\gamma \in \Gamma \mid \gamma, -\gamma < v(x) \ , \ \forall x \in \mathfrak{p}\}.$$

Esta correspondência reverte a inclusão e, em particular, se o posto de $\mathcal{O}$ *é finito então ele coincide com a dimensão de Krull de* $\mathcal{O}$.

Prova. Seja Δ um subgrupo convexo de Γ e mostremos que

$$\mathfrak{p}_\Delta = \{x \in K \mid v(x) > \delta \ , \ \forall \delta \in \Delta\},$$

é um ideal primo de $\mathcal{O}$.

De fato, pelas propriedades de valorização, é fácil ver que o conjunto $\mathfrak{p}_\Delta$ é um ideal de $\mathcal{O}$. Para comprovar que ele é também primo, suponhamos que existem $x, y \notin \mathcal{O}$ tais que $xy \in \mathfrak{p}_\Delta$. Então

$$v(xy) > \delta,$$

para todo $\delta \in \Delta$ enquanto que

$$v(x), v(y) \leq \delta_0$$

para algum $\delta_0 \in \Delta$; mas então

$$v(xy) = v(x) + v(y) \leq 2\delta_0 \in \Delta,$$

uma contradição. Concluímos assim que

$$xy \in \mathfrak{p}_\Delta \Rightarrow x \in \mathfrak{p}_\Delta \text{ ou } y \in \mathfrak{p}_\Delta.$$

Seja agora $\mathfrak{p}$ um ideal primo de $\mathcal{O}$ e mostremos que

$$\Delta_\mathfrak{p} = \{\gamma \in \Gamma \mid \gamma, -\gamma < v(x)\ ,\ \forall x \in \mathfrak{p}\},$$

é um subgrupo convexo de Γ.

De fato, a convexidade do conjunto $\Delta_\mathfrak{p}$ segue da sua definição. Também concluímos a partir dela que $-\Delta_\mathfrak{p} = \Delta_\mathfrak{p}$, de modo que falta-nos apenas mostrar que $\Delta_\mathfrak{p}$ é fechado para a adição. Ainda, como $\Delta_\mathfrak{p}$ é convexo e dois elementos de $\Delta_\mathfrak{p}$ são sempre comparáveis, para tal basta mostrar que

$$0 \leq \delta \in \Delta_\mathfrak{p} \Rightarrow \delta + \delta \in \Delta_\mathfrak{p}.$$

Suponha então que $\delta = v(x)$ para algum $x \in \mathcal{O}$ e que

$$v(x^2) = \delta + \delta \notin \Delta_\mathfrak{p},$$

ou seja, que

$$v(y) \leq v(x^2),$$

para algum $y \in \mathfrak{p}$. Então

$$x^2y^{-1} \in \mathcal{O} \overset{y \in \mathfrak{p}}{\Rightarrow} x^2 = x^2y^{-1}y \in \mathfrak{p} \overset{\mathfrak{p} \text{ é ideal primo}}{\Rightarrow} x \in \mathfrak{p} \Rightarrow \delta = v(x) \notin \Delta_\mathfrak{p},$$

uma contradição.

Facilmente verificamos que as aplicações explicitadas nas Afirmações 1 e 2 são inversas uma da outra, ou seja, para todo subgrupo convexo Δ de Γ e para todo ideal primo $\mathfrak{p}$ de $\mathcal{O}$,

$$\Delta = \Delta_{(\mathfrak{p}_\Delta)} \quad \text{e} \quad \mathfrak{p} = \mathfrak{p}_{(\Delta_\mathfrak{p})},$$

e que tal correspondência reverte a inclusão.

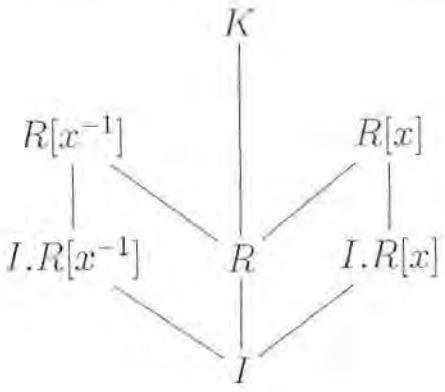
■

Como consequência direta do Lema 3.4.8 juntamente com o Corolário 3.4.7 e a Proposição 3.3.8 temos:

Corolário 3.4.9 *Se $\mathcal{O}$ é um anel de valorização não trivial de K então $\mathcal{O}$ tem posto 1 se, e somente se, $\mathcal{O}$ é um subanel maximal de K.*

Nosso objetivo agora é garantir a existência de anéis de valorização em um corpo arbitrário.

Proposição 3.4.10 *Sejam K um corpo, R um subanel de K e I um ideal próprio de R. Então, dado qualquer elemento não nulo $x \in K$, temos que $I.R[x]$ é um ideal próprio de $R[x]$ ou $I.R[x^{-1}]$ é um ideal próprio de $R[x^{-1}]$.*



Prova. Se assim não fosse teríamos que 1 se escreve nas seguintes formas:

$$\sum_{i=0}^{m} a_i x^i = 1 = \sum_{j=0}^{n} b_j x^{-j}$$

com $a_i, b_j \in I$ e m, n mínimais para esta propriedade. Daí:

- Se $m \geq n$, temos

$$\underbrace{(1-b_0)(1-a_0)}_{1-\underbrace{a_0-b_0+a_0b_0}_{\in I}} = (1-b_0)\sum_{i=1}^{m-1} a_i x^i + (1-b_0)a_m x^m$$

$$= (1-b_0)\sum_{i=1}^{m-1} a_i x^i + a_m x^m \sum_{j=1}^{n} b_j x^{-j}$$

$$= (1-b_0)\sum_{i=1}^{m-1} a_i x^i + \sum_{j=1}^{n} a_m b_j x^{m-j}$$

$$\Rightarrow 1 = a_0 + b_0 + a_0 b_0 + (1-b_0)\sum_{i=1}^{m-1} a_i x^i + \sum_{j=1}^{n} a_m b_j x^{m-j}$$

que é uma soma das potências $x^0, x, ..., x^{m-1}$, o que contraria o caráter minimal de m.

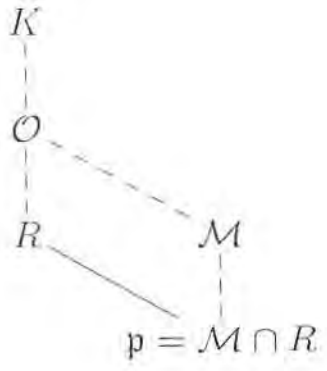
- A prova para o caso $m \leq n$ é similar.

■

Teorema 3.4.11 (Teorema da Extensão de Chevalley) *Fixados um corpo K, um subanel $R \subset K$ e um ideal primo $\mathfrak{p}$ de R, sempre existe um anel de valorização $\mathcal{O}$ de K tal que*

$$R \subset \mathcal{O} \quad e \quad \mathcal{M} \cap R = \mathfrak{p},$$

onde $\mathcal{M}$ é o ideal maximal de $\mathcal{O}$.



Prova. Sejam $R_{\mathfrak{p}}$ a localização de R por $\mathfrak{p}$ e

$$\Sigma = \left\{ (A, I) \;\middle|\; \begin{array}{l} A \text{ é um anel tal que } R_{\mathfrak{p}} \subseteq A \subseteq K \\ I \text{ é um ideal próprio de } A \text{ tal que } \mathfrak{p}R_{\mathfrak{p}} \subseteq I \subset A \end{array} \right\}.$$

Então $\Sigma \neq \emptyset$, pois $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}}) \in \Sigma$. Também Σ pode ser parcialmente ordenado da seguinte maneira: dados $(A_1, I_1), (A_2, I_2) \in \Sigma$, definimos

$$(A_1, I_1) \leq (A_2, I_2) \text{ se e só se } A_1 \subseteq A_2 \text{ e } I_1 \subseteq I_2.$$

É fácil verificar que cada subconjunto totalmente ordenado $\{(A_j, I_j) \mid j \in J\}$ de Σ, com $J \neq \emptyset$, tem uma cota superior em $(\Sigma, \leq)$, a saber,

$$\left(\bigcup_{j \in J} A_j, \bigcup_{j \in J} I_j \right).$$

Portanto, pelo Lema de Zorn, Σ tem pelo menos um elemento maximal, que vamos denotar por $(\mathcal{O}, \mathcal{M})$.

Assim,

$$R \subseteq R_{\mathfrak{p}} \subseteq \mathcal{O} \text{ e } \mathfrak{p}R_{\mathfrak{p}} \subseteq \mathcal{M} \subseteq \mathcal{O}.$$

Como $\mathfrak{p}R_{\mathfrak{p}}$ é o único ideal maximal de $R_{\mathfrak{p}}$ e está contido em $\mathcal{M}$, vale $\mathcal{M} \cap R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$, e então

$$\mathcal{M} \cap R = \mathfrak{p}.$$

Para completar a demonstração basta-nos mostrar que $\mathcal{O}$ é um anel de valorização.

- Pelo caráter maximal do par $(\mathcal{O}, \mathcal{M})$ temos que $\mathcal{M}$ é um ideal maximal de $\mathcal{O}$.

- Afirmamos que $\mathcal{O}$ é um anel local.

De fato, caso contrário existiria em $\mathcal{O}$ um elemento não invertível x que não pertence a $\mathcal{M}$. Pela Proposição 3.4.10, temos que $\mathcal{M}\mathcal{O}[x]$ é um ideal próprio de $\mathcal{O}[x]$ ou $\mathcal{M}\mathcal{O}[x^{-1}]$ é um ideal próprio de $\mathcal{O}[x^{-1}]$, ambos sobreanéis de $\mathcal{O}$.

Mas $\mathcal{O}[x] = \mathcal{O}$, já que $x \in \mathcal{O}$, daí segue que

$$\mathcal{M} \subsetneq \mathcal{M}\mathcal{O}[x] \subsetneq \mathcal{O},$$

absurdo, pois $\mathcal{M}$ é maximal.

Se $\mathcal{M}\mathcal{O}[x^{-1}]$ é um ideal próprio de $\mathcal{O}[x^{-1}]$ então teríamos

$$(\mathcal{O}[x^{-1}], \mathcal{M}\mathcal{O}[x^{-1}]) \in \Sigma$$

e está acima do elemento maximal $(\mathcal{O}, \mathcal{M})$, também um absurdo.

Assim, $\mathcal{M}$ é o único ideal maximal de $\mathcal{O}$.

- Afirmamos que $\mathcal{O}$ é um anel de valorização.

De fato, caso contrário teríamos um elemento $y \in K$ tal que $y, y^{-1} \notin \mathcal{O}$, e portanto

$$\mathcal{O} \subsetneq \mathcal{O}[y] \quad \text{e} \quad \mathcal{O} \subsetneq \mathcal{O}[y^{-1}].$$

Mas a Proposição 3.4.10 nos garante que $\mathcal{M}\mathcal{O}[y]$ é um ideal próprio de $\mathcal{O}[y]$ ou $\mathcal{M}\mathcal{O}[y^{-1}]$ é um ideal próprio de $\mathcal{O}[y^{-1}]$, o que, em qualquer caso, contraria o caráter maximal do par $(\mathcal{O}, \mathcal{M})$.

■

Aplicamos agora este teorema para caracterizar o fecho inteiro de um domínio D em um corpo K que o contém.

Teorema 3.4.12 *Fixado um corpo K,*

(1) *Todo anel de valorização $\mathcal{O}$ de K é um domínio integralmente fechado.*

(2) *Dado um subanel D de K, denotemos por $\mathbb{V}$ o conjunto de todos os anéis de valorização $\mathcal{O}$ de K com ideal maximal $\mathcal{M}$, tais que $D \subset \mathcal{O}$ e $\mathcal{M} \cap D$ é um ideal maximal de D. Então denotando por $\overline{D}$ o fecho inteiro de D em K, temos*

$$\overline{D} = \bigcap_{\mathcal{O} \in \mathbb{V}} \mathcal{O}.$$

Prova. (1) : Suponhamos que $x \in K$ é inteiro sobre $\mathcal{O}$, digamos,

$$a_0 + a_1 x + ... + a_{n-1} x^{n-1} + x^n = 0$$

para certos $a_0, ..., a_{n-1} \in \mathcal{O}$. Se $x \notin \mathcal{O}$ então $x^{-1} \in \mathcal{M}$, onde $\mathcal{M}$ denota o ideal maximal de $\mathcal{O}$; multiplicando a igualdade acima por x^{-n} obtemos

$$-1 = a_0 x^{-n} + ... + a_{n-1} x^{-1} \in \mathcal{M},$$

uma contradição. Assim, $x \in \mathcal{O}$.

(2) : Por (1) cada $\mathcal{O} \in \mathbb{V}$ é integralmente fechado em K, e então é claro que

$$\overline{D} \subset \bigcap_{\mathcal{O} \in \mathbb{V}} \mathcal{O}.$$

Reciprocamente, se $x \in K \backslash \overline{D}$ devemos verificar que $x \notin \bigcap_{\mathcal{O} \in \mathbb{V}} \mathcal{O}$. Garantimos isto encontrando um anel de valorização $\mathcal{O} \in \mathbb{V}$ tal que $x \notin \mathcal{O}$.

Observamos primeiramente que $x \notin \overline{D}[x^{-1}]$, pois senão

$$x = b_0 + b_1 x^{-1} + ... + b_m x^{-m},$$

para certos $b_0, ..., b_m \in \overline{D}$. Multiplicando a igualdade acima por x^m temos que x é inteiro sobre $\overline{D}$, e portanto $x \in \overline{D}$, uma contradição.

Consequentemente, x^{-1} não é invertível em $\overline{D}[x^{-1}]$, de modo que

$$x^{-1} \in m$$

para algum ideal maximal m de $\overline{D}[x^{-1}]$. Pelo Teorema de Chevalley (Teorema 3.4.11) existe um anel de valorização $\mathcal{O}$ de K com ideal maximal $\mathcal{M}$ tal que

$$\overline{D}[x^{-1}] \subset \mathcal{O} \quad \text{e} \quad \mathcal{M} \cap \overline{D}[x^{-1}] = m. \tag{21}$$

Assim $x^{-1} \in \mathcal{M}$, e então $x \notin \mathcal{O}$. Para mostrar que $\mathcal{O} \in \mathbb{V}$ falta ver que o ideal $\mathcal{M} \cap D$ de D é maximal.

Para isto, observamos que

$$\mathcal{M} \cap \overline{D} = \mathcal{M} \cap \overline{D}[x^{-1}] \cap \overline{D} \overset{(21)}{=} m \cap \overline{D}. \tag{22}$$

Mas $m \cap \overline{D}$ é um ideal maximal de $\overline{D}$, pois considerando a aplicação canônica

$$\varphi : \overline{D} \to \overline{D}[x^{-1}]/m,$$

temos que $\ker(\varphi) = m \cap \overline{D}$ e $\overline{D}[x^{-1}]/m$ é um corpo.

Assim, $m \cap D$ é ideal primo de D. Além disso, $D/(m \cap D)$ é tal que

$$\frac{D}{(m \cap D)} = \frac{D}{(m \cap \overline{D} \cap D)} \subseteq \frac{\overline{D}}{(m \cap \overline{D})}.$$

Do fato de $\overline{D}$ ser inteiro sobre D segue que $\overline{D}/(m \cap \overline{D})$ é uma extensão inteira de $D/(m \cap D)$. Por outro lado, $\overline{D}/(m \cap \overline{D})$ é corpo, de modo que $D/(m \cap D)$ é também corpo.

Assim, $m \cap D$ é um ideal maximal de D. Daí:

$$\mathcal{M} \cap D = (\mathcal{M} \cap \overline{D}) \cap D \overset{(22)}{=} (m \cap \overline{D}) \cap D = m \cap D,$$

e portanto $\mathcal{O} \in \mathbb{V}$.

■

Lema 3.4.13 *Sejam $\mathcal{O}_1, ..., \mathcal{O}_n$ anéis de valorização de K e $\mathcal{M}_1, ..., \mathcal{M}_n$ seus respectivos ideais maximais. Sejam*

$$R = \bigcap_{i=1}^{n} \mathcal{O}_i \quad e \quad \mathfrak{p}_i := R \cap \mathcal{M}_i.$$

Então

$$\mathcal{O}_i = R_{\mathfrak{p}_i},$$

para cada $i \in \{1, ..., n\}$.

Prova. $R_{\mathfrak{p}_i} \subseteq \mathcal{O}_i$, pois $R \subseteq \mathcal{O}_i$ e

$$s \in R \backslash (R \cap \mathcal{M}_i) \Rightarrow s \in \mathcal{O}_i \quad \text{e} \quad s \notin \mathcal{M}_i \Rightarrow s \in \mathcal{O}_i^{\times} \Rightarrow s^{-1} \in \mathcal{O}_i^{\times},$$

de modo que

$$\frac{a}{s} \in R_{\mathfrak{p}_i} \Rightarrow a \in R = \bigcap_{i=1}^{n} \mathcal{O}_i \quad \text{e} \quad s^{-1} \in \mathcal{O}_i^{\times} \Rightarrow \frac{a}{s} \in \mathcal{O}_i.$$

Para provar que $\mathcal{O}_i \subseteq R_{\mathfrak{p}_i}$ consideramos $a \in \mathcal{O}_i$, para um fixado i, e

$$I_a = \{j \mid a \in \mathcal{O}_j\}$$

Seja

$$\alpha_j = a + \mathcal{M}_j \in \mathcal{O}_j/\mathcal{M}_j =: K_j, \tag{23}$$

para cada $j \in I_a$. Escolhemos um número primo $p \in \mathbb{N}$ tal que, para todo $j \in I_a$,

$$p > \mathsf{car}(K_j) \quad \text{e} \quad \alpha_j \text{ não é uma raíz } p-\text{ésima da unidade 1.}$$

Então o elemento

$$b := 1 + a + ... + a^{p-1}.$$

é tal que

$$b \in \mathcal{O}_j,$$

para todo $j \in I_a$ e em K_j,

$$\overline{b} = \begin{cases} = \overline{1} + \overline{1} + .. + \overline{1} = \overline{p} \neq \overline{0}, \text{ se } a + \mathcal{M}_j = 1 + \mathcal{M}_j \\ \overset{(23)}{=} \overline{1} + \alpha_j + \alpha_j^2 + ... + \alpha_j^{p-1} = \frac{1-\alpha_j^p}{1-\alpha_j} \neq \overline{0}, \text{ se } a + \mathcal{M}_j \neq 1 + \mathcal{M}_j \end{cases}$$

de modo que, em qualquer caso, podemos afirmar que $b \in \mathcal{O}_j^{\times}$ para todo $j \in I_a$.

Para $j \in \{1, ..., n\} \backslash I_a$, temos $a \notin \mathcal{O}_j$, o que implica $a^{-1} \in \mathcal{M}_j$. Disto segue que

$$1 + a^{-1} + ... + a^{-(p-1)} \in \mathcal{O}_j^{\times},$$

e consequentemente,

$$b^{-1} = \frac{1}{a^{p-1}}\left(\frac{a^{p-1}+...+1}{a^{p-1}}\right)^{-1} = \underbrace{a^{-(p-1)}}_{\in \mathcal{M}_j}\ \underbrace{(1+a^{-1}+...+a^{-(p-1)})^{-1}}_{\in \mathcal{O}_j^\times} \in \mathcal{O}_j,$$

e também, pelo mesmo motivo,

$$ab^{-1} = a^{-(p-2)}(1+a^{-1}+...+a^{-(p-1)})^{-1} \in \mathcal{O}_j.$$

Portanto, para todo $1 \leq j \leq n$ mostramos que

$$b^{-1},\ ab^{-1} \in \mathcal{O}_j;$$

daí,

$$b^{-1}, ab^{-1} \in R$$

e, para aquele fixado i, uma vez que $b \in \mathcal{O}_i^\times$, temos

$$b^{-1} \notin \mathcal{M}_i \cap R = \mathfrak{p}_i,$$

e portanto

$$a = \frac{ab^{-1}}{b^{-1}} \in R_{\mathfrak{p}_i}.$$

■

Teorema 3.4.14 *Sejam $\mathcal{O}_1, ..., \mathcal{O}_n$ anéis de valorização de K e $\mathcal{M}_1, ..., \mathcal{M}_n$ seus respectivos ideais maximais. Sejam*

$$R = \bigcap_{i=1}^{n} \mathcal{O}_i \quad e \quad \mathfrak{p}_i := R \cap \mathcal{M}_i.$$

Suponhamos também que $\mathcal{O}_i \nsubseteq \mathcal{O}_j$ para todo $i \neq j$. Então:

(1) $\forall\ i \neq j\ ,\ \mathfrak{p}_i \nsubseteq \mathfrak{p}_j$;

(2) $\mathfrak{p}_1, ..., \mathfrak{p}_n$ *são todos os ideais maximais de* R;

(3) *para todo* $(a_1, ..., a_n) \in \mathcal{O}_1 \times .... \times \mathcal{O}_n$ *existe* $a \in R$ *com* $a - a_i \in \mathcal{M}_i$ *para todo* $i \in \{1, .., n\}$.

Prova. (1) Como $\mathfrak{p}_j := R \cap \mathcal{M}_j$, temos que, se existirem i, j tais que

$$\mathfrak{p}_i \subseteq \mathfrak{p}_j$$

então, pelo Lema 3.4.13

$$\mathcal{O}_j = R_{\mathfrak{p}_j} \subseteq R_{\mathfrak{p}_i} = \mathcal{O}_i.$$

(2) Basta-nos mostrar que todo ideal $I \neq R$ está contido em algum $\mathfrak{p}_i$ com $1 \leq i \leq n$. A fim de obter uma contradição, supomos que existe um ideal $I \neq R$ tal que, para todo $i \in \{1, .., n\}$, existe

$$a_i \in I \backslash \mathfrak{p}_i.$$

Por (1), para cada $i \neq j$, existe

$$b_{ij} \in \mathfrak{p}_i \backslash \mathfrak{p}_j.$$

Então, para todo $i \neq j$,

$$c_j := \prod_{i \neq j} b_{ij} \in \mathfrak{p}_i \backslash \mathfrak{p}_j.$$

Assim, fixado j, temos

$$a_j c_j \notin \mathfrak{p}_j \quad \text{e} \quad a_j c_j \in \mathfrak{p}_i,$$

para todo $i \neq j$

Logo, para todo $i \in \{1, .., n\}$,

$$d := \sum_{j=1}^{n} a_j c_j \in I \backslash \mathfrak{p}_i,$$

e portanto

$$d^{-1} \in R_{\mathfrak{p}_i} \overset{\text{Lema 3.4.13}}{=} \mathcal{O}_i,$$

para todo $i \in \{1, .., n\}$. Ou seja,

$$d^{-1} \in R = \bigcap_{i=1}^{n} \mathcal{O}_i,$$

e então

$$1 = d^{-1}.d \in I,$$

uma contradição.

(3) Para $i \neq j$ temos $\mathfrak{p}_i + \mathfrak{p}_j = R$ por (2) e (1). Portanto, pelo Teorema Chinês dos Restos, a aplicação canônica

$$R \longrightarrow R/\mathfrak{p}_1 \times ... \times R/\mathfrak{p}_n$$

é sobrejetora. Como

$$R/\mathfrak{p}_i \simeq R_{\mathfrak{p}_i}/\mathfrak{p}_i R_{\mathfrak{p}_i} \overset{\text{Lema 3.4.13}}{=} \mathcal{O}_i/\mathcal{M}_i,$$

temos que é sobrejetora a aplicação

$$R \longrightarrow \mathcal{O}_1/\mathcal{M}_1 \times ... \times \mathcal{O}_n/\mathcal{M}_n.$$

■

Observação 3.4.15 *A condição (3) do teorema diz que dados quaisquer elementos de $\mathcal{O}_1, ..., \mathcal{O}_n$, conseguimos encontrar em R um elemento suficientemente próximo destes.*

Encerramos esta seção mencionando um resultado sobre resultante de polinômios que será utilizado adiante.

Definição 3.4.16 *Sejam D um domínio e*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_0 \quad e \quad g(X) = b_m X^m + b_{m-1} X^{m-1} + ... + b_0$$

polinômios em $D[X]$ de graus m e n, ambos ≥ 1. A resultante de $f(X)$ e $g(X)$, denotada por $Res(f, g)$, é o elemento de D obtido pelo determinante

da matriz $(m+n)\times(m+n)$ *abaixo:*

$$Res(f,g) := \left|\begin{array}{ccccccc} a_n & a_{n-1} & \cdots & a_{m-1} & \cdots & a_0 & \\ & a_n & \cdots & \vdots & & \cdots & a_0 \\ & \vdots & & \vdots & & & \\ & \vdots & & a_n & \cdots & \cdots & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & & \\ & b_m & \cdots & \vdots & \cdots & b_1 & b_0 \\ & & & \vdots & & & \\ & & & \vdots & \cdots & \cdots & \\ & & & b_m & \cdots & \cdots & \cdots & b_0 \end{array}\right| \begin{array}{l} \left.\begin{array}{l}\\\\\\\end{array}\right\} m \text{ linhas} \\ \left.\begin{array}{l}\\\\\\\end{array}\right\} n \text{ linhas,} \end{array}$$

sendo que as posições não ocupadas por tais coeficientes são completadas com zeros (Salientamos que existem $m = \deg(g)$ *linhas de coeficientes de* f *e existem* $n = \deg(f)$ *linhas de coeficientes de* g*).*

O resultado a seguir salienta a utilidade da resultante.

Teorema 3.4.17 *Seja* D *um domínio e sejam* $f(X), g(X) \in D[X]$ *dois polinômios de grau* ≥ 1*.*

(a) Se $f(X)$ *e* $g(X)$ *possuem um fator comum em* $D[X]$ *de grau* ≥ 1*, então* $Res(f,g) = 0$*.*

(b) Se D *é um domínio fatorial e se* $Res(f,g) = 0$*, então* $f(X)$ *e* $g(X)$ *possuem um fator comum de grau* ≥ 1 *em* $D[X]$*.*

(c) Se

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_0;\ a_n \neq 0$$

$$e\ \ g(X) = b_mX^m + b_{m-1}X^{m-1} + ... + b_0;\ b_m \neq 0,$$

então a resultante $Res(f,g)$ *é uma soma de termos do tipo*

$$\pm\, a_{i_1}...a_{i_m}\ b_{j_1}...b_{j_n},\ \ com\ i_1 + ... + i_m + j_1 + ... + j_n = mn.$$

Prova. Ver [6].

■

Observação 3.4.18 *Se h' é a derivada formal de h, em particular obtemos de*

$$Res(h, h') \neq 0 \Rightarrow h \text{ e } h' \text{ não têm fator não constante em comum em } D[X];$$

em particular que h e h' não têm raíz comum em D, ou seja, $h(X)$ não tem raízes múltiplas em D.

Lema 3.4.19 *Suponha que K é um corpo com valorização v não trivial cujo grupo de valores é Γ. Então, para todo polinômio mônico*

$$g(X) = a_0 + a_1X + ... + a_{n-1}X^{n-1} + X^n \in K[X]$$

e todo $\gamma \in \Gamma$, existe um polinômio separável

$$h(X) = b_0 + b_1X + ... + b_{n-1}X^{n-1} + X^n \in K[X]$$

tal que

$$v(a_i - b_i) > \gamma,$$

para todo $0 \leq i \leq n$.

Prova. Sejam $Y_0, ..., Y_{n-1}$ indeterminadas sobre K. A partir de $g(X)$, construímos o polinômio

$$\begin{aligned} f_Y(X) &= f_{Y_0,...,Y_{n-1}}(X) \\ &= (a_0 + Y_0) + (a_1 + Y_1)X + ... + (a_{n-1} + Y_{n-1})X^{n-1} + X^n \\ &\in K(Y_0, ..., Y_{n-1})[X]. \end{aligned}$$

Consideramos agora a resultante $Res(f_Y(X), f'_Y(X))$ de f e de sua derivada formal f' com respeito à variável X no domínio $K[Y_0, ..., Y_{n-1}]$.

Como $Y_0, ...Y_{n-1}$ são algebricamente independentes sobre K, das propriedades da resultante temos que $Res(f_Y, f'_Y)$ é um polinômio não trivial $R(Y_0, ..., Y_{n-1}) \in K[Y_0, ..., Y_{n-1}]$.

Como já observado anteriormente, como v é não trivial temos que K não é um corpo finito. Logo, para todo $\gamma \in \Gamma$ o conjunto $\{x \in K \mid v(x) > \gamma\}$ tem um número infinito de elementos. Assim, existem $c_1, ..., c_{n-1} \in K$ com $v(c_i) > \gamma$ para os quais o polinômio resultante não se anula, isto é, $R(c_0, ..., c_{n-1}) \neq 0$. Portanto, tomando

$$h(X) = (a_0 + c_0) + (a_1 + c_1)X + ... + (a_{n-1})X^{n-1} + X^n,$$

segue que

$$Res(h, h') = Res(f_Y, f'_Y)(c_0, ..., c_{n-1}) = R(c_0, ..., c_{n-1}) \neq 0.$$

Disto concluímos, pelo Teorema 3.4.17, que h e h' não têm fator não constante em comum em $K[X]$; em particular, h e h' não têm raízes em comum, ou ainda, $h(X)$ não tem raízes múltiplas em K. Assim, $h(X)$ é um polinômio separável sobre K. É fácil constatar que $h(X)$ satisfaz as demais condições do lema.

■

3.5 Extensões de Corpos Valorizados

O objetivo desta seção é discutir quando e de quantas maneiras uma valorização v_1 de um corpo K_1 pode ser estendida a uma valorização de um corpo K_2 que contém K_1. Salientamos que a existência de ao menos um anel de valorização em K_2 é garantida pelo Teorema de Chevalley (Teorema 3.4.11), e portanto deve existir alguma valorização v_2 em K_2 que corresponde a este anel.

Começamos pela definição de extensão de valorizações e de extensão de anéis de valorização e tratamos de assegurar sua existência.

Definição 3.5.1 *Se K_1 é um subcorpo de K_2, v_1 é uma valorização sobre K_1 e v_2 é uma valorização sobre K_2, dizemos que v_2 extende v_1 ou que v_2 restringe-se a v_1 se $v_2|_{K_1} = v_1$.*

Definição 3.5.2 *Sejam $K_2|K_1$ uma extensão de corpos, $\mathcal{O}_1 \subseteq K_1$ e $\mathcal{O}_2 \subseteq K_2$ anéis de valorização. Dizemos que $\mathcal{O}_2$ é um prolongamento de $\mathcal{O}_1$ se*

$$\mathcal{O}_2 \cap K_1 = \mathcal{O}_1.$$

Escrevemos para isto simplesmente

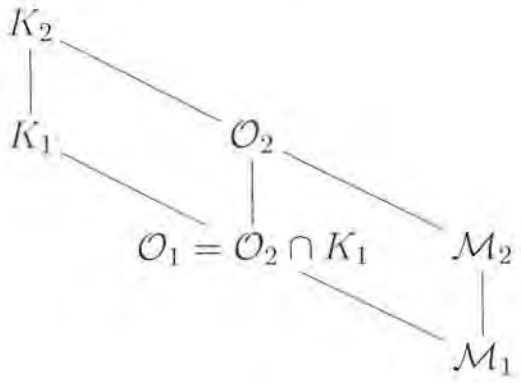
$$(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$$

Usamos também expressões como "$\mathcal{O}_2$ é uma extensão de $\mathcal{O}_1$", ou "$\mathcal{O}_2$ contrai sobre $\mathcal{O}_1$", para expressar que $\mathcal{O}_2$ é um prolongamento de $\mathcal{O}_1$.

Obviamente v_2 estende v_1 se e somente se $\mathcal{O}_2$ estende $\mathcal{O}_1$.

Observação 3.5.3 *Suponha $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ como acima. Sejam $\mathcal{M}_1$ e $\mathcal{M}_2$ os ideais maximais de $\mathcal{O}_1$ e $\mathcal{O}_2$, respectivamente. Então afirmamos que*

$$\mathcal{M}_2 \cap K_1 = \mathcal{M}_2 \cap \mathcal{O}_1 = \mathcal{M}_1 \quad e \quad \mathcal{O}_2^\times \cap K_1 = \mathcal{O}_2^\times \cap \mathcal{O}_1 = \mathcal{O}_1^\times.$$



Uma maneira de verificar isto é utilizando as valorizações v_1 e v_2 destes anéis e observando que $v_2|_{K_1} = v_1$, uma vez que $\mathcal{O}_1 = \mathcal{O}_2 \cap K_1$.

Para uma extensão de corpos $K_2|K_1$ e um anel de valorização $\mathcal{O}_2$ de K_2, vemos que $\mathcal{O}_1 = \mathcal{O}_2 \cap K_1$ também é um anel de valorização de K_1, e portanto $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$.

Teorema 3.5.4 *Sejam $K_2|K_1$ uma extensão de corpos e $\mathcal{O}_1 \subset K_1$ anel de valorização. Então existe uma extensão $\mathcal{O}_2$ de $\mathcal{O}_1$ a K_2.*

Prova. Como $\mathcal{O}_1$ é subanel de K_2, pelo Teorema de Chevalley (Teorema 3.4.11), existe um anel de valorização $\mathcal{O}_2$ de K_2 com $\mathcal{O}_1 \subset \mathcal{O}_2$ e $\mathcal{M}_2 \cap \mathcal{O}_1 = \mathcal{M}_1$. Mas $\mathcal{O}_2 \cap K_1$ e $\mathcal{O}_1$ têm o mesmo ideal maximal, portanto têm as mesmas unidades e então coincidem.

■

Como consequência do Teorema 3.4.12, obtemos

Corolário 3.5.5 *Sejam $K_2|K_1$ uma extensão de corpos, $\mathcal{O}_1$ um anel de valorização de K_1 e $\overline{\mathcal{O}_1}$ o fecho inteiro de $\mathcal{O}_1$ em K_2. Então*

$$\overline{\mathcal{O}_1} = \bigcap_{\substack{\mathcal{O}_2' \text{ é a.v. de } K_2 \\ \mathcal{O}_2' \cap K_1 = \mathcal{O}_1}} \mathcal{O}_2',$$

isto é, $\overline{\mathcal{O}_1}$ é a interseção de todos os prolongamentos de $\mathcal{O}_1$ a K_2.

Prova. Vamos aqui aplicar o Teorema 3.4.12. Seja $\mathcal{M}_1$ o ideal maximal de $\mathcal{O}_1$. Vimos que

$$\overline{\mathcal{O}_1} = \bigcap_{\mathcal{O}_2'' \in \mathbb{V}} \mathcal{O}_2'',$$

onde $\mathbb{V}$ é o conjunto de todos os anéis de valorização $\mathcal{O}_2''$ de K_2 com ideal maximal $\mathcal{M}_2''$, tais que $\mathcal{O}_1 \subset \mathcal{O}_2''$ e $\mathcal{M}_2'' \cap \mathcal{O}_1$ é um ideal maximal de $\mathcal{O}_1$, ou seja, $\mathcal{M}_1$.

($\supseteq$): Para cada prolongamento $\mathcal{O}_2'$ de $\mathcal{O}_1$ em K_2 seja $\mathcal{M}_2'$ seu ideal maximal. Então pela Observação 3.5.3,

$$\mathcal{M}_1 = \mathcal{M}_2' \cap \mathcal{O}_1$$

é o ideal maximal de $\mathcal{O}_1$. Assim $\{\mathcal{O}_2' \mid \mathcal{O}_2' \text{ é a.v. de } K_2 \text{ e } \mathcal{O}_2' \cap K_1 = \mathcal{O}_1\} \subseteq \mathbb{V}$.

($\subseteq$): Se $\mathcal{O}_2'$ é um anel de valorização de K_2 contendo $\mathcal{O}_1$ com ideal maximal $\mathcal{M}_2'$ satisfazendo

$$\mathcal{M}_2' \cap \mathcal{O}_1 = \mathcal{M}_1,$$

então

$$\mathcal{O}_2' \cap K_1 = \mathcal{O}_1.$$

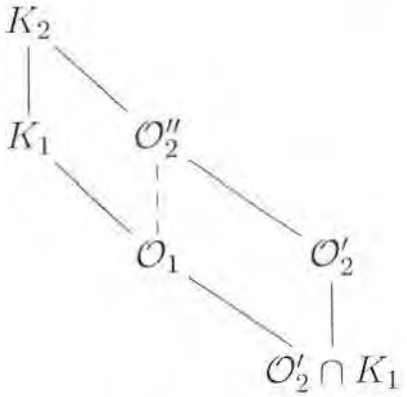
Com isto, mostramos que $\{\mathcal{O}_2' \mid \mathcal{O}_2' \text{ é a.v. de } K_2 \text{ e } \mathcal{O}_2' \cap K_1 = \mathcal{O}_1\} \supseteq \mathbb{V}$ e que vale a igualdade das interseções.

■

Proposição 3.5.6 *Sejam $K_2|K_1$ extensão de corpos e $\mathcal{O}_2'$ um anel de valorização em K_2. Então todo anel de valorização $\mathcal{O}_1$ de K_1 que satisfaz*

$$\mathcal{O}_1 \supseteq \mathcal{O}_2' \cap K$$

pode ser estendido a algum anel de valorização $\mathcal{O}_2'' \supseteq \mathcal{O}_2'$ de K_2.



Prova. Sejam respectivamente Γ_2' e v_2' o grupo de valores e a valorização associados a $\mathcal{O}_2'$ e $\Gamma \subset \Gamma_2'$ o grupo de valores de $\mathcal{O}_2' \cap K_1$. Pelo Corolário 3.4.7 e pelo Lema 3.4.8, o anel de valorização $\mathcal{O}_1$ corresponde a um subgrupo convexo $\Delta \subseteq \Gamma$ e, mais precisamente, se denotamos por v a valorização correspondente a $\mathcal{O}_2' \cap K_1$, então

$$\mathcal{O}_1 = (\mathcal{O}_2' \cap K_1)_{\mathfrak{p}_\Delta} = \{x \in K_1 \mid v(x) \geq \delta \text{ para algum } \delta \in \Delta\}.$$

Ao definirmos

$$\mathcal{O}_2'' = \{x \in L \mid v_2'(x) \geq \delta \text{ para algum } \delta \in \Delta\},$$

temos obviamente $\mathcal{O}_2' \subset \mathcal{O}_2''$ $(v_2'|_{K_1} = v)$ e

$$\begin{aligned}\mathcal{O}_2'' \cap K_1 &= \{x \in K_1 \mid v_2'(x) \geq \delta \text{ para algum } \delta \in \Delta\} \\ &= \{x \in K_1 \mid v(x) \geq \delta \text{ para algum } \delta \in \Delta\} = \mathcal{O}_1,\end{aligned}$$

e então $\mathcal{O}_2''$ é o desejado anel de valorização.

■

O resultado a seguir mostra como os grupos de valores e os corpos de restos se relacionam em uma extensão de corpos valorizados:

Proposição 3.5.7 *Seja $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ uma extensão arbitrária de corpos valorizados. Para cada $\mathcal{O}_i$, com $i \in \{1, 2\}$, seja*

$$v_i : K_i \twoheadrightarrow \Gamma_i \cup \{\infty\}$$

a valorização associada a $\mathcal{O}_i$. Então:

i) o grupo ordendo Γ_1 é ordem-isomorfo a um subgrupo ordenado de Γ_2;

ii) o corpo de resíduos $\overline{K_1}$ associado a v_1 é isomorfo a um subcorpo do corpo de resíduos $\overline{K_2}$ associado a v_2.

Prova. *i)* De fato, lembramos que

$$v_i|_{K_i^\times} : K_i^\times \twoheadrightarrow \Gamma_i$$

é um homomorfismo de grupos (um multiplicativo e o outro aditivo), com núcleo $\mathcal{O}_i^\times$ e portanto

$$K_i^\times / \mathcal{O}_i^\times \cong \Gamma_i.$$

Mais ainda, a aplicação composta da inclusão com a projeção canônica

$$K_1^\times \overset{i}{\hookrightarrow} K_2^\times \twoheadrightarrow K_2^\times / \mathcal{O}_2^\times \cong \Gamma_2$$

tem núcleo

$$\mathcal{O}_2^\times \cap K_1^\times = \mathcal{O}_1^\times;$$

donde concluímos:

$$\Gamma_1 \cong K_1^\times/\mathcal{O}_1^\times \hookrightarrow K_2^\times/\mathcal{O}_2^\times \cong \Gamma_2.$$

ii) Denotando os respectivos ideais maximais por $\mathcal{M}_1$ e $\mathcal{M}_2$, a aplicação composta

$$\mathcal{O}_1 \overset{i}{\hookrightarrow} \mathcal{O}_2 \twoheadrightarrow \mathcal{O}_2/\mathcal{M}_2 = \overline{K_2}$$

tem núcleo

$$\mathcal{M}_2 \cap \mathcal{O}_1 \overset{\text{Obs. 3.5.3}}{=} \mathcal{M}_1.$$

Logo,

$$\overline{K_1} = \mathcal{O}_1/\mathcal{M}_1 \hookrightarrow \mathcal{O}_2/\mathcal{M}_2 = \overline{K_2}.$$

■

O resultado acima nos diz que podemos considerar Γ_1 como um subgrupo ordenado de Γ_2, bem como o corpo de resíduos $\overline{K_1}$ como um subcorpo de $\overline{K_2}$. Desta forma, faz sentido a seguinte

Definição 3.5.8 *Seja $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ uma extensão arbitrária de corpos valorizados, e sejam Γ_1 e Γ_2 os correspondentes grupos ordenados e corpos residuais satisfazendo $\Gamma_1 \subset \Gamma_2$ e $\overline{K}_1 \subset \overline{K}_2$.*

Chamamos respectivamente os números

$$e := e(\mathcal{O}_2|\mathcal{O}_1) := [\Gamma_2 : \Gamma_1]$$

e

$$f := f(\mathcal{O}_2/\mathcal{O}_1) := [\overline{K_2} : \overline{K_1}]$$

de índice de ramificação e grau residual (ou grau de inércia) da extensão $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ (ou simplesmente $K_2|K_1$, quando são claros os anéis de valorização que estamos considerando).

Se $e(\mathcal{O}_2/\mathcal{O}_1) = 1$ e $f(\mathcal{O}_2/\mathcal{O}_1) = 1$ então dizemos que a extensão

$$(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$$

é imediata.

Exemplo 3.5.9 *O completamento* $(\widehat{K}, \mathcal{O}_{\widehat{v}})$ *de um corpo valorizado* $(K, \mathcal{O}_v)$ *de posto 1, é uma extensão imediata pelo Teorema 3.2.19, enquanto que a extensão apresentada no Teorema 3.5.13 não é imediata se escolhermos* $\gamma \notin \Gamma$.

Observação 3.5.10 *O índice de ramificação e o grau residual são multiplicativos, ou seja, se* $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2) \subseteq (K_3, \mathcal{O}_3)$ *são extensões de corpos valorizados, então*

$$e(\mathcal{O}_3/\mathcal{O}_1 = e(\mathcal{O}_3/\mathcal{O}_2)e(\mathcal{O}_2/\mathcal{O}_1) \quad e \quad f(\mathcal{O}_3/\mathcal{O}_1) = f(\mathcal{O}_3/\mathcal{O}_2)f(\mathcal{O}_2/\mathcal{O}_1).$$

O resultado a seguir mostra como os índices de ramificação e grau de inércia de uma extensão de corpos valorizados se relacionam com o grau da extensão.

Proposição 3.5.11 *Sejam* $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ *uma extensão de corpos valorizados e*

$$v_i : K_i \twoheadrightarrow \Gamma_i \cup \{\infty\}$$

as valorizações correspondentes a $\mathcal{O}_i$ *para* $i \in \{1, 2\}$. *Sejam* $e = e(\mathcal{O}_2/\mathcal{O}_1)$ *e* $f = f(\mathcal{O}_2/\mathcal{O}_1)$. *Escolhemos* $\omega_1, ..., \omega_f \in \mathcal{O}_2$ *e* $\pi_1, ..., \pi_e \in K_2^\times$ *tais que:*

(1) $\overline{\omega_1}, ..., \overline{\omega_f} \in \overline{K_2}$ *são linearmente independentes sobre* $\overline{K_1}$;

(2) $v_2(\pi_1), ..., v_2(\pi_e)$ *são representantes das classes laterais distintas de* Γ_2/Γ_1.

Então, para todo $a_{ij} \in K_1$,

$$v_2\left(\sum_{i=1}^{f}\sum_{j=1}^{e} a_{ij}\omega_i\pi_j\right) = \min\{v_2(a_{ij}\omega_i\pi_j) \mid 1 \leq i \leq f \ , \ 1 \leq j \leq e\}.$$

Em particular, os elementos do conjunto $\{\omega_i\pi_j \mid 1 \leq i \leq f \ e \ 1 \leq j \leq e\}$ *são linearmente independentes sobre* K_1, *e portanto*

$$e.f \leq [K_2 : K_1].$$

Prova. Sejam $a_{ij} \in K_1$ não todos nulos e sejam $I \in \{1, ..., f\}$ e $J = \{1, ..., e\}$ tais que

$$v_2(a_{IJ}\pi_J) = \min\{v_2(a_{ij}\pi_j) \mid (i,j) \in \{1, ..., f\} \times \{1, ..., e\}\}$$

Afirmação : Para todo $j \neq J$ vale

$$v_2(a_{IJ}\pi_J) < v_2(a_{ij}\pi_j).$$

pois caso contrário teríamos igualdade para algum $j \neq J$, e neste caso

$$v_2(\pi_J) - v_2(\pi_j) = v_2(a_{ij}) - v_2(a_{IJ}) \in \Gamma_1,$$

o que contradiz o fato de que $v_2(\pi_J)$ e $v_2(\pi_j)$ são representantes de classes laterais distintas de Γ_2/Γ_1.

Suponhamos por absurdo que

$$z = \sum_{i=1}^{f}\sum_{j=1}^{e} a_{ij}\omega_i\pi_j \quad \text{e} \quad v_2(z) > \min\{v_2(a_{ij}\omega_i\pi_j) \mid 1 \leq i \leq f\ ,\ 1 \leq j \leq e\}.$$

Então, pela Afirmação e pela hipótese $\omega_1, ..., \omega_f \in \mathcal{O}_2$, temos

$$v_2(z) > v_2(a_{IJ}\pi_J) \Rightarrow v_2(z(a_{IJ}\pi_J)^{-1}) > 0 \Rightarrow z(a_{IJ}\pi_J)^{-1} \in \mathcal{M}_2$$

e, novamente pela Afirmação,

$$a_{ij}\pi_j(a_{IJ}\pi_J)^{-1} \in \mathcal{M}_2,$$

para todo $j \neq J$. Daí, como $\omega_1, ..., \omega_f \in \mathcal{O}_2$,

$$\sum_{\substack{j=1 \\ j\neq J}}^{e}\sum_{i=1}^{f} a_{ij}\pi_j(a_{IJ}\pi_J)^{-1}\omega_i \in \mathcal{M}_2$$

Então, de

$$\underbrace{z(a_{IJ}\pi_J)^{-1}}_{\in\mathcal{M}_2} = \underbrace{\sum_{\substack{j=1\\ j\neq J}}^{e}\sum_{i=1}^{f} a_{ij}\pi_j(a_{IJ}\pi_J)^{-1}\omega_i}_{\in\mathcal{M}_2} + \sum_{i=1}^{f} a_{iJ}\pi_J(a_{IJ}\pi_J)^{-1}\omega_i,$$

concluímos que

$$\sum_{i=1}^{f} a_{iJ}\pi_J(a_{IJ}\pi_J)^{-1}\omega_i \in \mathcal{M}_2 \overset{a_{iJ}\pi_J(a_{IJ}\pi_J)^{-1}\in\mathcal{O}_2}{\Rightarrow} \overline{0} = \sum_{i=1}^{f} \overline{a_{iJ}(a_{IJ})^{-1}}\,\overline{\omega_i},$$

sendo o coeficiente de $\overline{\omega_I} = \overline{1} \neq \overline{0}$, o que contradiz a hipótese de serem $\overline{\omega_1}, ..., \overline{\omega_f} \in \overline{K_2}$ linearmente independentes sobre $\overline{K_1}$, uma vez que $\overline{a_{iJ}(a_{IJ})^{-1}}$ são até elementos de $\mathcal{O}_1/\mathcal{M}_2 \cap K_1 = \mathcal{O}_1/\mathcal{M}_1 = \overline{K_1}$.

É fácil convencer-se que os elementos do conjunto $\{\omega_i\pi_j \mid 1 \leq i \leq f \text{ e } 1 \leq j \leq e\}$ são linearmente independentes sobre K_1.

■

3.5.1 A Extensão Transcendente $K(X)|K$

Nesta seção, resumimo-nos a estudar com mais detalhe a extensão $K(X)|K$, apresentando algumas maneiras de construir valorizações em $K(X)$ que prolongam uma dada valorização em K. Começamos com um resultado preliminar:

Lema 3.5.12 *Seja D um domínio. Se existe uma aplicação*

$$v : D \twoheadrightarrow \Gamma \cup \{\infty\},$$

onde Γ é um grupo abeliano totalmente ordenado, satisfazendo as condições

(*i*) $v(a) = \infty \Leftrightarrow a = 0$.

(*ii*) $v(ab) = v(a) + v(b)$.

(*iii*) $v(a+b) \geq \inf\{v(a), v(b)\}$.

então v dá origem a uma valorização

$$w : K \twoheadrightarrow \Gamma \cup \{\infty\}$$

com $K = cf(D)$, simplesmente definindo

$$w\left(\frac{a}{b}\right) = v(a) - v(b).$$

Prova. A aplicação

$$w : K \twoheadrightarrow \Gamma \cup \{\infty\}$$

está bem definida. De fato, se $a_1/b_1 = a_2/b_2$, com $a_1, b_1, a_2, b_2 \in D$, então $a_1 b_2 = a_2 b_1$. Logo,

$$v(a_1) + v(b_2) = w(a_1 b_2) = w(a_2 b_1) = v(a_2) + v(b_1),$$

e então,

$$w\left(\frac{a_1}{b_1}\right) = v(a_1) - v(b_1) = v(a_2) - v(b_2) = w\left(\frac{a_2}{b_2}\right).$$

Falta estender as propriedades de valorização de D para K. Sejam $c_1, c_2 \in K\backslash\{0\}$. Tome c como um denominador comum de c_1 e c_2, ou seja, tal que $c_i = a_i/c$ para $i \in \{1, 2\}$ com $a_1, a_2, c \in D$. Portanto

$$\begin{aligned} w(c_1 + c_2) = w(\tfrac{a_1+a_2}{c}) &= w(a_1 + a_2) - w(c) \\ &\geq \min\{w(a_1), w(a_2)\} - w(c) \\ &= \min\{w(a_1) - w(c), w(a_2) - w(c)\} \\ &= \min\{w(c_1), w(c_2)\}. \end{aligned}$$

$$\begin{aligned} w(c_1 c_2) = w(\tfrac{a_1 a_2}{c^2}) &= w(a_1 a_2) - w(c^2) \\ &= w(a_1) - w(c) + w(a_2) - w(c) \\ &= w(c_1) + w(c_2). \end{aligned}$$

■

Teorema 3.5.13 *Dados um subgrupo ordenado Γ de um grupo ordenado*

Γ', *uma valorização*

$$v : K \twoheadrightarrow \Gamma \cup \{\infty\}$$

e $\gamma \in \Gamma'$, *definimos, dado* $f = \sum_{i=0}^{n} a_i X^i \in K[X]$,

$$w(f) := \begin{cases} \infty & , \text{ se } f = 0 \\ \min\limits_{0 \le i \le n} \{v(a_i) + i\gamma\}, & \text{caso contrário} \end{cases}$$

e, para $g = \sum_{j=0}^{m} b_j X^j \in K[X] \backslash \{0\}$,

$$w(f/g) := w(f) - w(g).$$

Então $w : K(X) \to \Gamma' \cup \{\infty\}$ *é uma valorização em* $K(X)$ *que estende* v *e cujo grupo de valores é* $w(K(X)^\times) = \Gamma + \gamma\mathbb{Z} \subset \Gamma'$.

$$\begin{array}{ccccc} K(X) & \xrightarrow{w} & \Gamma + \gamma\mathbb{Z} & \hookrightarrow & \Gamma' \\ \downarrow & & \downarrow & & \\ K & \xrightarrow{v} & \Gamma & & \end{array}$$

Prova. Supondo já mostrado que w é uma valorização verificamos que o seu grupo de valores é $\Gamma + \gamma\mathbb{Z}$. De fato é claro que $w(X) = \gamma$. E pela definição de w, se $\delta \in w(K(X)^\times)$ então existem $f, g \in K[X] \backslash \{0\}$ tais que

$$\begin{aligned} \delta &= w\left(\frac{f}{g}\right) = w(f) - w(g) \\ &= \min_{0 \le i \le n} \{v(a_i) + i\gamma\} - \min_{0 \le j \le m} \{v(b_j) + j\gamma\} \in \Gamma + \gamma\mathbb{Z}, \end{aligned}$$

e disto temos $w(K(X)^\times) \subseteq \Gamma + \gamma\mathbb{Z}$. Agora, dado $\gamma' + \gamma n \in \Gamma + \gamma\mathbb{Z}$ com $n \in \mathbb{Z}$, $x \in K \backslash \{0\}$ tal que $v(x) = \gamma'$, temos que $f = cX^n \in K(X)$ é tal que $w(f) = \gamma' + \gamma n$.

Passamos agora para a verificação de que a aplicação w realmente define uma valorização. Pelo Lema 3.5.12, basta testarmos (i), (ii) e (iii) para os elementos de $K[X]$.

- Dados $f, g \in K[X]$, é claro que $w(f+g) \ge \min\{w(f), w(g)\}$ e $w(fg) = w(f) + w(g)$ se f ou g for o polinômio nulo. Assim, podemos supor $f, g \in$

$K[X]\backslash\{0\}$. Pondo $n = \max\{\deg(f), \deg(g)\}$, podemos escrever, sem perda de generalidade,

$$f = \sum_{i=0}^{n} a_i X^i \quad \text{e} \quad g = \sum_{i=0}^{n} b_i X^i;$$

com $a_i, b_i \in K$, de modo que

$$w(f+g) = \min_{0\leq i\leq n} \{v\,(a_i + b_i) + i\gamma\}.$$

Para cada $j \in \{0, 1, ..., n\}$ temos

$$\begin{aligned} v(a_j + b_j) + j\gamma &\geq \min_{0\leq i\leq n} \{v(a_i), v(b_i)\} + i\gamma \\ &= \min_{0\leq i\leq n} \{v(a_i) + i\gamma, v(b_i) + i\gamma\} \geq \min\{w(f), w(g)\} \end{aligned}$$

em particular,

$$w(f+g) \geq \min\{w(f), w(g)\}.$$

- Agora mostramos que $w(f.g) = w(f) + w(g)$.

Escrevendo

$$f = \sum_{i=0}^{n} a_i X^i \quad \text{e} \quad g = \sum_{j=0}^{m} b_j X^j,$$

temos

$$f.g = \sum_{k=0}^{n+m} c_k X^k, \quad \text{com} \quad c_k = \sum_{i+j=k} a_i b_j.$$

Se $i + j = k$ então

$$w(a_i b_j X^k) = v(a_i) + v(b_j) + k\gamma = v(a_i) + i\gamma + v(b_j) + j\gamma \geq w(f) + w(g).$$

Assim,

$$\begin{aligned} w(c_k X^k) = v(c_k) + k\gamma &\geq \min\{v(a_i b_j) \mid i + j = k\} + k\gamma \\ &= \min\{v(a_i b_j) + k\gamma \mid i + j = k\} \geq w(f) + w(g), \end{aligned}$$

donde concluímos

$$w(f.g) = \min_{0\leq k\leq m+n} \{v(c_k) + k\gamma\} \geq w(f) + w(g).$$

Para mostrar que na verdade vale até a igualdade, mostramos que vale a desigualdade contrária. Tomamos

$$\begin{cases} i_0 = \min\{i \mid v(a_i) + i\gamma = w(f)\} \\ j_0 = \min\{j \mid v(b_j) + j\gamma = w(g)\} \\ k_0 = i_0 + j_0 \end{cases}$$

Claramente vale

$$c_{k_0} = \sum_{i+j=k_0} a_i b_j = \sum_{\substack{i+j=k_0 \\ i<i_0}} a_i b_j + a_{i_0} b_{i_0} + \sum_{\substack{i+j=k_0 \\ i>i_0}} a_i b_j.$$

No primeiro termo da soma temos sempre $i < i_0$, e portanto, pelo caráter minimal de i_0 e pela definição de i_0 e de w, temos para tais índices

$$v(a_i) + i\gamma > w(f).$$

Logo, em cada termo $a_i b_j$ do primeiro somatório

$$v(a_i b_j) + k_0\gamma \overset{i+j=k_0}{=} \underbrace{v(a_i) + i\gamma}_{>w(f)} + \underbrace{v(b_j) + j\gamma}_{\geq w(g)} > w(f) + w(g).$$

Por simetria, já que $i + j = k_0$ e $i > i_0$ implica $j < j_0$, podemos aplicar no último somatório o mesmo raciocínio e obter a mesma desigualdade para $i > i_0$. Consequentemente

$$\begin{aligned} v\Big(\sum_{\substack{i+j=k_0 \\ i<i_0}} a_i b_j\Big) &> w(f) + w(g) - k_0\gamma \\ &= v(a_{i_0}) + i_0\gamma + v(b_{j_0}) + j_0\gamma - k_0\gamma \\ &= v(a_{i_0}) + v(b_{j_0}) = v(a_{i_0} b_{i_0}), \end{aligned}$$

e analogamente

$$v\Big(\sum_{\substack{i+j=k_0 \\ i>i_0}} a_i b_j\Big) > v(a_{i_0}, b_{i_o}).$$

Concluímos assim, pelo Corolário 3.2.12, que

$$v(c_{k_0}) = v(a_{i_0}b_{i_0}),$$

e então $v(c_{k_0}) + k_0\gamma = w(f) + w(g)$ pela definição de i_0 e j_0. Donde segue que

$$w(f.g) \leq v(c_{k_0}) + k_0\gamma = w(f) + w(g).$$

Finalmente

$$w(f.g) = w(f) + w(g).$$

■

Salientamos que a valorização w construída no resultado acima prescreve $w(X) = \gamma$. A valorização considerada no próximo Corolário é comumente conhecida como a extensão de Gauss da valorização v em K ao corpo de funções racionais $K(X)$: ela prescreve não só $w(X) = 0$ como também $\overline{X}$ transcendente sobre $\overline{K}$.

Corolário 3.5.14 *Suponha que $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ é uma valorização sobre K. Então existe exatamente uma extensão w de v a $K(X)$ tal que $w(X) = 0$ e $\overline{X}$ é transcendente sobre $\overline{K}$. Para tal w, temos $\overline{K(X)} = \overline{K}(\overline{X})$ e $w(K(X)^\times) = \Gamma$, a saber*

$$w(\sum_{i=0}^{n} a_i X^i) = \min_{0\leq i\leq n} v(a_i).$$

Prova. Provemos inicialmente a unicidade: sejam $f = \sum_{i=0}^{n} a_i X^i \in K[X]\backslash\{0\}$ e $k \leq n$ tal que

$$v(a_k) = \min_{0\leq i\leq n} v(a_i).$$

Como obviamente $a_k \neq 0$, podemos escrever

$$f = a_k \underbrace{\sum_{i=0}^{n} b_i X^i}_{=:g}, \text{ onde } b_i = \frac{a_i}{a_k} \text{ e } v(b_i) \geq 0. \tag{24}$$

Então $w(g) \geq 0$, já que $w(X) = 0$. Além disto,

$$\overline{g} = \sum_{i=0}^{n} \overline{b_i}.\overline{X}^{\,i} \neq \overline{0},$$

já que $b_k = 1$ e $\overline{X}$ é transcendente sobre $\overline{K}$. Portanto

$$g \in \mathcal{O}_w^{\times}, \quad \text{e então} \quad w(g) = 0,$$

donde

$$w(f) = w(a_k) + w(g) \overset{w(g)=0 \text{ e } w|_K=v}{=} v(a_k) = \min_{0\leq i\leq n} v(a_i).$$

Ou seja, é precisamente a valorização definida no Teorema 3.5.13 se lembrarmos que aqui $w(X) = 0$.

Para provar a existência definimos $w(f)$, para cada $f \in K[X]$, como no Teorema 3.5.13 com $\Gamma' = \Gamma$ e $\gamma = 0$, ou seja, $w(X) = 0$.

Afirmamos que, com esta definição, $\overline{X}$ é transcendente sobre $\overline{K}$. De fato, se

$$\sum_{i=0}^{n} \overline{a_i}\ \overline{X}^{\,i} = \overline{0}$$

para certos $a_i \in \mathcal{O}_v$, então

$$0 < w\left(\sum_{i=0}^{n} a_i X^i\right) = \min_{0\leq i\leq n} v(a_i),$$

e então $v(a_i) > 0$ para cada i, ou seja, $\overline{a_i} = 0$ como queríamos provar.

Claramente, pelo Teorema 3.5.13

$$w(K(X)^{\times}) = \Gamma.$$

Finalmente, afirmamos que $\overline{K(X)} = \overline{K}(\overline{X})$. Como $\overline{X}$ é transcendente sobre $\overline{K}$, é claro que $(\overline{X}) \subseteq \overline{K(X)}$. Para provar a recíproca, seja

$$h = \frac{f_1}{f_2} \in \mathcal{O}_w^{\times},$$

com $f_1, f_2 \in K[X]\backslash\{0\}$. Escrevemos, para $i \in \{1,2\}$,

$$f_i = c_i g_i$$

onde $c_i \in K^\times$ e $g_i \in \mathcal{O}_w^\times$ como em (24). Assim

$$h = \frac{c_1 g_1}{c_2 g_2} = c\frac{g_1}{g_2},$$

onde $c = c_1/c_2 \in K^\times$. Também temos $c \in \mathcal{O}_w^\times$ pois $h \in \mathcal{O}_w^\times$, e como foi visto, $w(g_i) = 0$, para $i \in \{1,2\}$. Finalmente,

$$\overline{h}.\overline{g_2} = \overline{c}.\overline{g_1} = \overline{cg_1} \in \overline{K}[\overline{X}] \;\Rightarrow\; \frac{\overline{cg_1}}{\overline{g_2}} \in \overline{K}(\overline{X}).$$

■

Observação 3.5.15 *Observamos que usando a valorização de Gauss para a extensão $K(X)|K$ apresentada no Corolário 3.5.14, a última condição do Lema 3.4.19 pode ser reescrita como*

$$w(g - f) > \gamma,$$

uma vez que $w(X) = 0$ e

$$w\left(\Sigma_{i=0}^{s} c_i X^i\right) = \min_{0\le i\le s} v(c_i).$$

Isto significa que o conjunto dos polinômios separáveis e mônicos é denso no conjunto dos polinômios mônicos com relação à valorização dada pela extensão de Gauss.

Corolário 3.5.16 *Sejam $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ uma valorização no corpo K, sendo Γ um subgrupo ordenado de um grupo ordenado Γ'. Se no Teorema 3.5.13 escolhemos $\gamma \in \Gamma'$ tal que*

$$n \in \mathbb{Z} \quad e \quad n\gamma \in \Gamma \;\Rightarrow\; n = 0.$$

então w é a única valorização de $K(X)$ que estende v e satisfaz $w(X) = \gamma$.

Esta valorização é tal que $\overline{K(X)} = \overline{K}$ *e* $w(K(X)^\times) = \Gamma \oplus \gamma\mathbb{Z}$ *com a ordem induzida por* Γ'.

Prova. A existência é garantida pelo Teorema 3.5.13.

Para a unicidade tome w uma extensão satisfazendo $w(X) = \gamma$.

Afirmamos que se $i \neq j$ e $a_i, a_j \in K^\times$, então $w(a_iX^i) \neq w(a_jX^j)$.

De fato,

$$w(a_iX^i) = w(a_jX^j) \Rightarrow v(a_i)+i\gamma = v(a_j)+j\gamma \Rightarrow (i-j)\gamma = v(a_j)-v(a_i) \in \Gamma,$$

e da hipótese sobre γ concluímos $i - j = 0$. Disto segue que

$$w(f) = \min\{w(a_0), ..., w(a_nX^n)\} = \min_{0\leq i\leq n}(v(a_i) + i\gamma),$$

o que implica a unicidade de w em $K[X]$ e portanto, pelo Lema 3.5.12, em $K(X)$.

É óbvio que $w(K(X)^\times) = w(K(X)\backslash\{0\}) = \Gamma \oplus \gamma\mathbb{Z}$, sendo a soma direta pela escolha de γ.

Falta-nos mostrar que $\overline{K(X)} = \overline{K}$.

Afirmação 1: Se $f \in K[X]\backslash\{0\}$ então f é da forma $f = aX^m(1 + u)$ com $a \in K^\times$, $m \in \mathbb{N}$ e $u \in K(X)$ com $w(u) > 0$.

Para isto escreva $f = \sum_{i=0}^{n} a_iX^i$ com $a_i \in K$. Vimos na prova do Teorema 3.5.13 que existe exatamente um i_0 tal que

$$w(f) = v(a_{i_0}) + i_0\gamma = w(a_{i_0}X^{i_0}).$$

Portanto

$$f = a_{i_0}X^{i_0}(1 + \sum_{\substack{i=0 \\ i\neq i_0}}^{n} \frac{a_iX^i}{a_{i_0}X^{i_0}}) = 1 + u.$$

Observando que para $i \neq i_0$

$$w\left(\frac{a_iX^i}{a_{i_0}X^{i_0}}\right) = w(a_iX^i) - w(a_{i_0}X^{i_0}) > 0,$$

concluímos que $w(u) > 0$.

Note que isto implica

$$w(1+u) = 0,$$

ou seja, $1+u$ é invertível em $\mathcal{O}_w$.

Afirmação 2: Valem as conclusões análogas para $h = \frac{f}{g} \in K(X)\backslash\{0\}$. Mais precisamente, h é da forma $h = cX^r(1+u")$ com $a \in K^\times$, $m \in \mathbb{Z}$ e $u" \in K(X)$ com $w(u") > 0$.

De fato, pela afirmação anterior, podemos escrever

$$f = aX^m(1+u) \quad \text{e} \quad g = bX^n(1+u'),$$

com $a, b \in K^\times$, $m, n \in \mathbb{N}$ e $w(u) > 0$, $w(u') > 0$. Então

$$h = \frac{f}{g} = \frac{a}{b}X^{m-n}\left(\frac{1+u}{1+u'}\right),$$

onde $c = a/b \in K^\times$ e $r = m - n \in \mathbb{Z}$. Ainda, como

$$\frac{1+u}{1+u'} = 1 + \frac{u-u'}{1+u}$$

e

$$w(u-u') \geq \min\{w(u), w(-u')\} > 0 = w(1+u'),$$

temos

$$w\left(\frac{u-u'}{1+u}\right) > 0.$$

e com isto concluímos que existem $c \in K^\times$, $r \in \mathbb{Z}$ e $u'' \in K(X)$ com $w(u'') > 0$ tais que

$$h = cX^r(1+u''). \tag{25}$$

Agora mostramos que $\overline{K(X)} = \overline{K}$: dado $h \in \mathcal{O}_w^\times$ escrito na forma (25), temos:

$$\begin{array}{lllll} 0 = w(h) & = & w(cX^r(1+u'')) & & \\ & \overset{w(1+u'')=0}{=} & w(cX^r) & \overset{w|_K=v \text{ e } w(X)=\gamma}{=} & v(c)+r\gamma \\ & \Rightarrow & \gamma = -v(c) \in \Gamma & \overset{\text{hipótese sobre } \gamma}{\Rightarrow} & r=0 \Rightarrow v(c)=0. \end{array}$$

Por outro lado, em $\overline{K(X)}$

$$\begin{aligned} \overline{h} &\overset{(25)}{=} \overline{cX^r(1+u'')} \overset{r=0}{=} \\ &= \overline{c}(\overline{1}+\overline{u''}) = \overline{c} \in \overline{K}, \end{aligned}$$

pois $w(u'') > 0$ implica $\overline{u''} = 0$.

■

Encerramos esta seção enunciando um resultado que envolve extensões transcendentes e extensões algébricas, mas que para o caso algébrico só precisamos da Proposição 3.5.7 e do Lema 3.5.12.

Lema 3.5.17 *Seja $(F, \mathcal{O})$ um corpo valorizado que não admite nenhuma extensão algébrica própria imediata.*[4] *Seja v' uma extensão de $v = v_\mathcal{O}$ sobre o corpo de funções racionais $F' = F(t)$, tal que:*

$$\forall\ a \in F,\ \exists\ b \in F \text{ com } v'(t-a) = v'(b) = v(b) \text{ e } \overline{(t-a)b^{-1}} \in \overline{F}. \quad (26)$$

Então v' é uma extensão imediata de v e os valores $v'(t-a)$ para $a \in F$ determinam v' univocamente.

Prova.

Provemos inicialmente que a extensão v' de v é imediata.

Afirmação: Para todo polinômio $f(t) \in F[t]$, existe $b \in F$ satisfazendo

$$v'(f(t)) = v(b) \quad \text{e} \quad \overline{f(t)b^{-1}} \in \overline{F}. \quad (27)$$

[4] Um tal corpo é chamado *corpo algebricamente maximal*, veja Definição 3.6.10

Note que, uma vez provada a *Afirmação 1*,

$$v'(F(t)) = v(F) \quad \text{e} \quad \overline{F'} = \overline{F}.$$

De fato, tomando $g, f \in F[t]$ com $g \neq 0$ e

$$\overline{\left(\frac{f}{g}\right)} \in \overline{F'},$$

existem $b_1, b_2 \in F$ tais que

$$v'(f) = v(b_1) \quad , \quad v'(g) = v(b_2)$$

e também

$$\overline{fb_1^{-1}} \quad , \quad \overline{gb_2^{-1}} \in \overline{F}.$$

Portanto

$$\overline{\left(\frac{f}{g}\right)} = \frac{\overline{(fb_1^{-1})}}{\overline{(gb_2^{-1})}} \, \overline{\left(\frac{b_1}{b_2}\right)} \in \overline{F}.$$

Provamos a *Afirmação* por indução sobre o grau de f, que vamos supor igual a n.

- a validade para $n = 1$ é garantida pela hipótese.

- seja $n \geq 2$ e suponhamos que (27) vale para todo polinômio f de grau $< n$.

- se f é redutível sobre F e $\deg(f) = n$ então obtemos (27) a partir da hipótese de indução que

$$f = g.h \ \text{ ambos de grau } \leq n - 1$$

implica

$$v'(f) = v'(g) + v'(h) \overset{\text{Hip. Ind.}}{=} v(b_1) + v(b_2) = v(b_1 b_2) \in v(F).$$

e

$$\overline{g(t)b_1^{-1}} \in \overline{F} \ \text{ e } \ \overline{h(t)b_2^{-1}} \in \overline{F} \ \Rightarrow \ \overline{f(t)(b_1 b_2)^{-1}} = \overline{g(t)h(t)(b_1 b_2)^{-1}} \in \overline{F}.$$

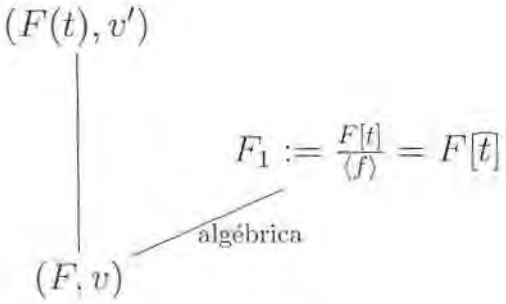
- se f é irredutível sobre F, restringimos inicialmente a valorização v' ao $F-$subespaço vetorial

$$V = F + Ft + ... + Ft^{n-1}.$$

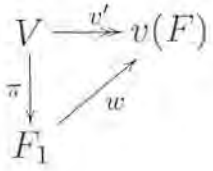
obtendo uma aplicação sobrejetora

$$v'|_V : V \to v'(V)$$

com $v'(V) = v(F)$ pela hipótese de indução e pelo fato de $F \subset V$. Observando o diagrama



onde $\overline{t} = t + \langle f \rangle$, temos assim sugerida uma aplicação w



dada por

$$w(a_0 + a_1\overline{t} + ... + a_{n-1}(\overline{t})^{n-1}) = v'(a_0 + a_1 t ... + a_{n-1}t^{n-1}).$$

que afirmamos estar bem definida: dados $g_1, g_2 \in F[t]$ e supondo

$$g_1 = q_1 f + r_1 \quad \text{e} \quad g_2 = q_2 f + r_2,$$

temos

$$g_1 + \langle f \rangle = g_2 + \langle f \rangle \Leftrightarrow r_1 = r_2.$$

Daí, neste caso,

$$w(g_1 + \langle f \rangle) = w(r_1 + \langle f \rangle) = v'(r_1) = v'(r_2) = w(r_2 + \langle f \rangle) = w(g_2 + \langle f \rangle).$$

Além disso w é sobrejetiva e satisfaz as seguintes propriedades (veja Lema 3.5.12):

(i) $w(g_1 + \langle f \rangle) = \infty \Leftrightarrow g_1 + \langle f \rangle = 0 + \langle f \rangle$,

(iii) $w(g_1 + \langle f \rangle + g_2 + \langle f \rangle) \geq \inf\{w(g_1 + \langle f \rangle, w(g_2) + \langle f \rangle\}$.

De fato, basta observar que

$$\begin{aligned} w(g_1 + \langle f \rangle) = \infty &\Leftrightarrow w(r_1 + \langle f \rangle) = \infty \\ &\Leftrightarrow v'(r_1) = \infty \\ &\Leftrightarrow r_1 = 0 \\ &\Leftrightarrow g_1 + \langle f \rangle = 0 + \langle f \rangle ; \end{aligned}$$

$$\begin{aligned} w(g_1 + \langle f \rangle + g_2 + \langle f \rangle) &= w(r_1 + r_2 + \langle f \rangle) \\ &= v'(r_1 + r_2) \\ &\geq \inf\{v'(r_1), v'(r_2)\} \\ &= \inf\{w(g_1 + \langle f \rangle, w(g_2) + \langle f \rangle\}. \end{aligned}$$

Assim, para w ser uma valorização no corpo $F_1 = F[\,\overline{t}\,]$, que é extensão algébrica própria de F, só faltaria mostrar (ii):

$$w((g_1 + \langle f \rangle)(g_2 + \langle f \rangle)) = w(g_1 + \langle f \rangle) + w(g_2 + \langle f \rangle) \qquad (28)$$

No entanto, se isto ocorresse afirmamos que teríamos como corpo de resíduos de F_1 determinado por w precisamente $\overline{F}$. Ou seja: para cada $g + \langle f \rangle \in F_1$, satisfazendo $w(g + \langle f \rangle) = 0$ existe $b \in F$ com $v(b) = 0$ e tal que $\overline{g + \langle f \rangle} = \overline{b}$ em $\overline{F_1}$, isto é,

$$w((g + \langle f \rangle)b^{-1}) = 0.$$

De fato, dado $g_1 + \langle f \rangle \in F_1$ com $w(g_1 + \langle f \rangle) = 0$, isto é, $v'(r_1) = 0$ onde

$$g_1 = qf_1 + r_1 \ , \ \ r_1 \in V;$$

temos, da hipótese de indução, que

$$\exists b_{g_1} \in F \text{ tal que } v'(r_1) = v'(b_{g_1}) = v(b_{g_1}) \text{ e } \overline{r_1 b_{g_1}^{-1}} \in \overline{F}.$$

Mas como $v'(r_1) = 0$, pela Proposição 3.5.7, temos que $\overline{r_1}$ faz sentido em $\overline{F} \subset \overline{F_1}$, e então podemos escrever

$$\overline{r_1}\ \overline{b_{g_1}^{-1}} = \overline{r_1 b_{g_1}^{-1}} \in \overline{F} \overset{b_{g_1} \in F}{\Rightarrow} \overline{r_1} \in \overline{F}$$

Como o grupo de valores de w também coincide com o grupo de valores de v, concluiríamos que a extensão algébrica $(F_1, w)|(F, v)$ (que é própria pois tem grau $n \geq 2$) é uma extensão imediata, o que contraria a hipótese sobre (F, v).

Assim, concluímos que w não pode satisfazer (28), e portanto existem polinômios $r_1, r_2, r \in V$ tais que

$$r_1 r_2 = qf + r \text{ para algum } q \in F[t], \tag{29}$$

e então

$$\begin{aligned} v'(r) &= w(r + \langle f \rangle) \overset{(29)}{=} w((r_1 + \langle f \rangle)(r_2 + \langle f \rangle)) \\ &\neq w(r_1 + \langle f \rangle) + w(r_2 + \langle f \rangle) = v'(r_1) + v'(r_2), \end{aligned}$$

Daí:

$$\begin{array}{ll} v'(f) & \overset{(29)}{=} \quad v'(r_1 r_2 - r) - v'(q) \\ & \overset{v'(r_1)+v'(r_2)\neq v'(r)}{=} \inf\{v'(r_1) + v'(r_2), v'(r)\} - v'(q) \end{array} \tag{30}$$

Usamos agora a hipótese de indução para os polinômios $r_1, r_2, r, q \in V$ para concluírmos a prova da *Afirmação 1*

Sejam $b_1, b_2, b, c \in F$ tais que

$$\begin{aligned} v'(r_1) = v(b_1) &\quad \text{e} \quad \overline{r_1 b_1^{-1}} \in \overline{F} \\ v'(r_2) = v(b_2) &\quad \text{e} \quad \overline{r_2 b_2^{-1}} \in \overline{F} \\ v'(r) = v(b) &\quad \text{e} \quad \overline{r b^{-1}} \in \overline{F} \\ v'(q) = v(c) &\quad \text{e} \quad \overline{q c^{-1}} \in \overline{F} \end{aligned}$$

Então temos, de (30),

$$v'(f) = \inf\{v(b_1) + v(b_2), v(b)\} - v(c) \tag{31}$$

Caso 1 : $\inf\{v(b_1) + v(b_2), v(b)\} = v(b_1) + v(b_2) = v(b_1 b_2)$.

Neste caso, (31) se reescreve como

$$v'(f) = v(b_1 b_2) - v(c) = v\left(\frac{b_1 b_2}{c}\right),$$

e também,

$$\overline{f.\left(\tfrac{b_1 b_2}{c}\right)^{-1}} = \overline{\tfrac{(r_1 r_2 - r)}{q}}.\ \overline{\tfrac{(b_1 b_2)^{-1}}{c^{-1}}}$$

$$= \overline{\tfrac{1}{(qc^{-1})}}.\left[\overline{r_1 b_1^{-1}}.\ \overline{r_2 b_2^{-1}} - \overline{rb^{-1}}.\ \overline{b}.\ \overline{(b_1 b_2)^{-1}}\right] \in \overline{F}.$$

Caso 2 : $\inf\{v(b_1) + v(b_2), v(b)\} = v(b)$.

Neste caso, (31) se reescreve como

$$v'(f) = v(b) - v(c) = v\left(\frac{b}{c}\right).$$

Daí

$$\overline{f\left(\frac{b}{c}\right)^{-1}} = \overline{\frac{r_1 r_2 - r}{q}}.\ \overline{\frac{b^{-1}}{c^{-1}}} = \overline{\frac{1}{(qc^{-1})}}\left[\overline{r_1 b_1^{-1}}.\ \overline{b_1}.\ \overline{r_2 b_2^{-1}}.\ \overline{b_2}.\ \overline{b^{-1}} - \overline{rb^{-1}}\right] \in \overline{F}$$

A igualdade (30) também nos mostra que $v'(f)$ fica muito bem determinada a partir do conhecimento de v' sobre polinômios de grau menor do que o de f (note que $r_1, r_2, r \in V$ e $r_1 r_2 = qf + r$ implica $q \in V$), que, por sua vez, dependeram apenas do conhecimento de v' sobre os polinômios de grau 1. Com isto está provada a segunda afirmação do enunciado.

■

3.5.2 Extensões Algébricas de Corpos Valorizados

Na Seção 3.2 vimos que, para uma valorização de posto 1 de um corpo K_1 (mais precisamente, para um valor absoluto de K_1), existe uma extensão de v_1 para o seu completamento $\widehat{K_1}$. Se $K_2 = K_1(X)$, também já sabemos construir algumas extensões de v_1 a uma valorização de K_2, como as feitas em 3.5.1. Concentramo-nos agora em extensões algébricas de corpos valorizados $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$. Neste caso, o conjunto

$$\mathbb{V} = \{\text{extensões de } \mathcal{O}_1 \text{ a } K_2\}$$

pode não ser finito (o que só pode ocorrer numa extensão infinita $K_2|K_1$ — veja Teorema 3.5.27); mostramos aqui que a sua cardinalidade é sempre limitada pelo grau de separabilidade de K_2 sobre K_1. Em particular, isto implica que $\mathbb{V}$ tem apenas um elemento para extensões puramente inseparáveis. Mostramos também que dois elementos distintos de $\mathbb{V}$ nunca são comparáveis pela inclusão, e que, se K_2 é uma extensão normal de K_1 os elementos de $\mathbb{V}$ são sempre K_1−conjugados, ou seja, são isomorfos através de algum $\sigma \in Aut(K_2|K_1)$.

Começamos com alguns fatos gerais para esta situação:

Teorema 3.5.18 *Seja $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ uma extensão de corpos valorizados sendo $K_2|K_1$ algébrica. Então:*

(1) *Para todo $\gamma \in \Gamma_2$ existe $n \in \mathbb{N}$ tal que $n\gamma \in \Gamma_1$, ou seja, Γ_2/Γ_1 é um grupo de torção.*

(2) *$\overline{K_2}$ é também uma extensão algébrica de $\overline{K_1}$.*

Prova. Dividimos em dois casos:

1°caso: $K_2|K_1$ é uma extensão finita: neste caso, a Proposição 3.5.11 nos garante que

$$e = e(\mathcal{O}_2/\mathcal{O}_1) = [\Gamma_2 : \Gamma_1] \quad \text{e} \quad f = f(\mathcal{O}_2/\mathcal{O}_1) = [\overline{K_2} : \overline{K_1}]$$

são também finitos, o que completa a prova.

2^ocaso: $K_2|K_1$ é uma extensão infinita: neste caso, para provar (1), tomamos $x \in K_2$ tal que $v_2(x) = \gamma \in \Gamma_2$. Sejam $L = K_1(x)$, $\mathcal{O} = \mathcal{O}_2 \cap L$ e $v = v_2|_L$ a restrição de v_2 a L. Tome $\Gamma = v(L^\times) \subset \Gamma_2$. Como $L|K_1$ é finita, pelo primeiro caso o quociente Γ/Γ_1 é um grupo finito. Assim, como $\gamma \in \Gamma$, existe um $n \in \mathbb{N}$ tal que $n\gamma \in \Gamma_1$. Para provar (2) supomos ainda que $x \in \mathcal{O}_2^\times$. Por argumento análogo, concluímos que o corpo de resíduos $\overline{L}$ é uma extensão finita de $\overline{K_1}$. Portanto $\overline{x} \in \overline{L} \subset \overline{K_2}$ é algébrico sobre $\overline{K_1}$.

■

Corolário 3.5.19 *Para toda extensão de corpos valorizados $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ com $K_2|K_1$ algébrica, os respectivos grupos de valores Γ_2 e Γ_1 (e portanto também $\mathcal{O}_2$ e $\mathcal{O}_1$) têm o mesmo posto.*

Prova. Consideremos a aplicação

$$\varphi : \{\text{subgrupos convexos de } \Gamma_2\} \to \{\text{subgrupos convexos de } \Gamma_1\},$$

$$\varphi(\Delta) = \Delta \cap \Gamma_1$$

Afirmamos que φ está bem definida e é bijetiva, o que nos permite concluir que Γ_2 e Γ_1 têm o mesmo posto.

De fato, é claro que φ está bem definida. Suponhamos agora que

$$\Delta \cap \Gamma_1 = \Delta' \cap \Gamma_1$$

e que existe

$$\gamma \in \Delta \backslash \Delta'.$$

Sem perda de generalidade podemos supor $\gamma \geq 0$. Pelo Teorema 3.5.18 existe $n \in \mathbb{N}$ com

$$n\gamma = \gamma' \in \Gamma_1 \cap \Delta = \Gamma_1 \cap \Delta',$$

já que $K_2|K_1$ é por hipótese algébrica.

Como Δ' é subgrupo convexo e $0 \leq \gamma \leq n\gamma$, temos $\gamma \in \Delta'$, um absurdo. Portanto $\Delta \subseteq \Delta'$. Trocando os papéis de Δ e Δ' concluímos também que $\Delta' \subseteq \Delta$, e então φ é injetora.

Dado $\Delta^* \subset \Gamma_1$ subgrupo convexo, vale

$$\Delta^* = \{\delta \in \Gamma_1 \mid \delta, -\delta \leq \gamma \text{ para algum } \gamma \in \Delta^*\}.$$

Portanto, existe um subgrupo convexo de Γ_2 tal que $\varphi(\Delta) = \Delta^*$, a saber,

$$\Delta = \{\delta \in \Gamma_2 \mid \delta, -\delta \leq \gamma \text{ para algum } \gamma \in \Delta^*\},$$

e então φ é sobrejetora.

■

Lema 3.5.20 *Se $K_2|K_1$ é uma extensão algébrica então nenhum anel de valorização não trivial de K_2 contém K_1.*

Prova. Sejam $\mathcal{O}_2$ um anel de valorização de K_2 que contém K_1 e $\alpha \in K_2$. Como $K_2|K_1$ é algébrica, existe o polinômio minimal de α sobre K_1, que vamos supor da forma

$$X^n + a_{n-1}X^{n-1} + ... + a_0,$$

com $a_0, ..., a_{n-1} \in K_1 \subset \mathcal{O}_2$. Mas então α é inteiro sobre $\mathcal{O}_2$, e portanto $\alpha \in \mathcal{O}_2$, uma vez que $\mathcal{O}_2$ é integralmente fechado.

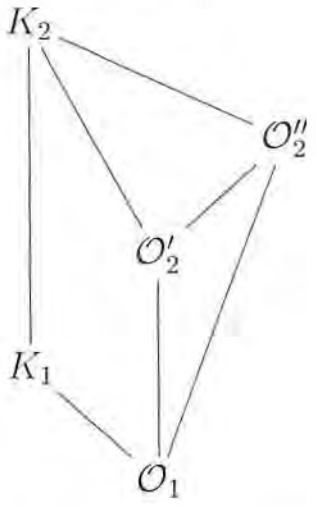
Assim, concluímos que $\mathcal{O}_2 = K_2$, o que completa a prova.

■

Observação 3.5.21 *Salientamos que o resultado acima não vale para extensões transcendentes: basta considerar o Exemplo 3.2.24: lá qualquer a.v. de $K(X)$ contém K, e no entanto não necessariamente coincide com $K(X)$.*

Lema 3.5.22 *Sejam $K_2|K_1$ uma extensão algébrica de corpos, $\mathcal{O}_1$ um anel de valorização de K_1 e $\mathcal{O}_2'$, $\mathcal{O}_2''$ anéis de valorização de K_2, ambos esten-*

dendo $\mathcal{O}_1$. *Se* $\mathcal{O}_2' \subseteq \mathcal{O}_2''$ *então* $\mathcal{O}_2' = \mathcal{O}_2''$.



Prova. Como $\mathcal{O}_2' \subseteq \mathcal{O}_2'' \subseteq K_2$, temos, pela Proposição 3.4.5(i),

$$\mathcal{M}_2'' \subseteq \mathcal{M}_2', \tag{32}$$

onde $\mathcal{M}_2'', \mathcal{M}_2'$ são os ideais maximais de $\mathcal{O}_2''$ e $\mathcal{O}_2'$, respectivamente.

Em particular, faz sentido o quociente $\mathcal{O}_2'/\mathcal{M}_2''$ como subconjunto de $\mathcal{O}_2''/\mathcal{M}_2''$ e que vamos denotar por $\overline{\mathcal{O}}_2'$. Assim, temos

$$\mathcal{O}_2' \to \overline{\mathcal{O}}_2' = \mathcal{O}_2'/\mathcal{M}_2'' \hookrightarrow \mathcal{O}_2''/\mathcal{M}_2''$$

Como $\mathcal{O}_2'$ é anel de valorização de K_2, é fácil ver que $\overline{\mathcal{O}}_2'$ é um anel de valorização de $\mathcal{O}_2''/\mathcal{M}_2''$, que vamos denotar simplesmente por $\mathcal{K}$; em particular, $\mathcal{K}$ é o corpo de frações de $\overline{\mathcal{O}}_2'$ pela Observação 3.4.6.

Como $\mathcal{O}_2''$ é uma extensão de $\mathcal{O}_1$, já sabemos que

$$\mathcal{M}_2'' \cap K_1 = \mathcal{M}_1,$$

de modo que existe um monomorfismo natural

$$\mathcal{O}_1/\mathcal{M}_1 \hookrightarrow \mathcal{O}_2'/\mathcal{M}_2''.$$

Portanto

$$\overline{K}_1 = \mathcal{O}_1/\mathcal{M}_1 \hookrightarrow \overline{\mathcal{O}}_2' = \mathcal{O}_2'/\mathcal{M}_2'' \hookrightarrow \mathcal{O}_2''/\mathcal{M}_2'' = \mathcal{K};$$

com certo abuso de notação, podemos simplesmente escrever

$$\overline{K}_1 \subseteq \overline{\mathcal{O}}'_2 \subseteq \mathcal{K}.$$

Mas então $\overline{\mathcal{O}}'_2$ é um anel de valorização de $\mathcal{K}$ que contém o corpo $\overline{K}_1$. Como, pelo Teorema 3.5.18, $\mathcal{K}|\overline{K}_1$ é uma extensão algébrica, temos, pelo Lema 3.5.20,

$$\overline{\mathcal{O}}'_2 = \mathcal{K}.$$

Ou seja,

$$\mathcal{O}'_2/\mathcal{M}''_2 = \overline{\mathcal{O}}'_2 = \mathcal{K} = \mathcal{O}''_2/\mathcal{M}''_2. \tag{33}$$

o que, junto com (32), nos permite concluir que

$$\mathcal{O}''_2 = \mathcal{O}'_2,$$

pois

$$\begin{aligned} a \in (\mathcal{O}''_2)^\times &\overset{(33)}{\Rightarrow} \exists b \in \mathcal{O}'_2, \quad a + \mathcal{M}''_2 = b + \mathcal{M}''_2 \\ &\Rightarrow a - b \in \mathcal{M}''_2 \overset{(32)}{\subseteq} \mathcal{M}'_2 \\ &\Rightarrow a \in b + \mathcal{M}'_2 \subseteq \mathcal{O}'_2. \end{aligned}$$

■

Dadas uma extensão algébrica $K_2|K_1$ e um anel de valorização $\mathcal{O}_1$ de K_1, podem existir infinitos anéis de valorização de K_2 estendendo $\mathcal{O}_1$. Contudo, às vezes este número de extensões tem um limite. Antes de abordarmos alguns destes casos, relembramos algumas definições, notações e resultados da Teoria de Corpos. (Maiores detalhes sobre eles podem ser encontrados em [10] ou em [7]).

Definição 3.5.23 *A partir daqui, denotamos por $\widetilde{K}$ um fecho algébrico de K. Dado um corpo K, denotamos por K^s o fecho separável de K, isto é*

$$K^s = \{x \in \widetilde{K} \mid x \text{ é separável sobre } K\}.$$

Se $car(K) = 0$ então $K^s = \widetilde{K}$; se $car(K) = p > 0$ e x é algébrico sobre K então existe $k \in \mathbb{N}$ tal que

$$x^{p^k} \text{ é separável sobre } K.$$

Dada uma extensão algébrica $K_2|K_1$, o conjunto

$$K_2 \cap K_1^s = \{x \in K_2 \mid x \text{ é separável sobre } K_1\}.$$

é um corpo e é uma extensão separável de K_1.

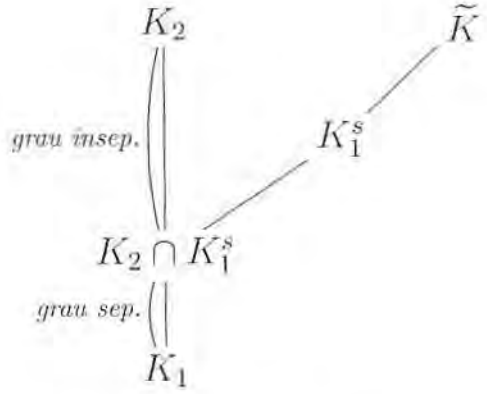
Definição 3.5.24 *Dada uma extensão algébrica $K_2|K_1$, o número*

$$[K_2 : K_1]_s = [K_2 \cap K_1^s : K_1]$$

é chamado o grau de separabilidade de K_2 sobre K_1. E o número

$$[K_2 : K_1]_i = [K_2 : K_2 \cap K_1^s]$$

é chamado o grau de inseparabilidade de K_2 sobre K_1.



Da Teoria de Corpos temos então que

$$[K_2 : K_1] = [K_2 : K_1]_s \, [K_2 : K_1]_i,$$

uma vez que

$$K_1 \subseteq K_1^s \cap K_2 \subseteq K_2.$$

Definição 3.5.25 *Dizemos que uma extensão algébrica $K_2|K_1$ é puramente*

inseparável quando

$$K_2 \cap K_1^s = K_1,$$

ou, equivalentemente,

$$[K_2 : K_1]_s = 1.$$

Definição 3.5.26 *Um corpo K é dito um corpo separavelmente fechado se a extensão $\widetilde{K}|K$ é puramente inseparável.*

Teorema 3.5.27 *Seja $K_2|K_1$ uma extensão algébrica tal que*

$$[K_2 : K_1]_s < \infty.$$

Se $\mathcal{O}_1$ é um anel de valorização de K_1 então o número de prolongamentos de $\mathcal{O}_1$ a K_2 é finito e limitado por $[K_2 : K_1]_s$.

Prova. Sejam $\mathcal{O}_1, ..., \mathcal{O}_m$ alguns prolongamentos distintos de $\mathcal{O}_1$ a K_2 com respectivos ideais maximais $\mathcal{M}_1, ..., \mathcal{M}_m$. O Lema 3.5.22 nos assegura que estes prolongamentos são incomparáveis dois a dois. Assim, o Teorema 3.4.14(3) se aplica, e nos garante que existem

$$c_1, ..., c_m \in R = \bigcap_{i=1}^{n} \mathcal{O}_i$$

tais que para todo $j \in \{1, ..., m\}$, $c_j \in R$ está próximo de $1 \in \mathcal{O}_j$ e de $0 \in \mathcal{O}_i$, para todo $i \neq j$. Ou seja, para todo $j \in \{1, ..., m\}$,

$$c_j - 1 \in \mathcal{M}_j \quad \text{e} \quad c_i \in \mathcal{M}_j,$$

para todo $i \neq j$, com $i \in \{1, ..., m\}$. Daí:

Afirmação 1: Se os corpos têm característica zero, afirmamos que $c_1, ..., c_m$ são linearmente independentes sobre K_1, e portanto

$$m \leq [K_2 : K_1] = [K_2 : K_1]_s.$$

Se os corpos têm característica $p > 0$, sabemos que, para cada $i \in \{1, ..., m\}$ existe um natural k_i tal que

$$c_i^{p^{k_i}} \text{ é separável sobre } K_1,$$

o mesmo ocorrendo para todo natural maior do que k_i. Assim, existe $k \in \mathbb{N}$ tal que $c_1^{p^k}, ..., c_m^{p^k}$ são separáveis sobre K_1.

Afirmação 2: O elementos $c_1^{p^k}, ..., c_m^{p^k} \in K_2 \cap K_1^s$ são linearmente independentes sobre K_1 (e portanto $m \leq [K_2 : K_1]_s$).

A prova da Afirmação 1 pode ser obtida da prova da Afirmação 2, apenas substituindo p^k por 1. Esta, por sua vez, é provada por contradição: suponhamos que $a_1, ..., a_m \in K_1$ são não todos nulos e tais que

$$\sum_{i=0}^{m} a_i c_i^{p^k} = 0.$$

Tomamos j tal que $1 \leq j \leq m$ e $v(a_j) = \min\{v(a_1), ..., v(a_m)\}$. Então $a_j \neq 0$, pois senão seriam todos nulos, e

$$c_j^{p^k} = -\sum_{i \neq j} a_j^{-1} a_i {c_i}^{p^k} \in \mathcal{M}_j.$$

Isto implica $c_j \in \mathcal{M}_j$ e $c_j - 1 \in \mathcal{M}_j$, donde obtemos $1 \in \mathcal{M}_j$, um absurdo.

Com isto obtemos $m \leq [K_2 : K_1]_s$.

■

Corolário 3.5.28 *Suponha que K_2 é uma extensão algébrica puramente inseparável de K_1. Então todo anel de valorização $\mathcal{O}_1$ de K_1 tem uma única extensão a K_2. Em particular, se K_1 é um corpo separavelmente fechado, então todo anel de valorização $\mathcal{O}_1$ de K_1 tem uma única extensão ao seu fecho algébrico $\widetilde{K_1}$.*

Prova. Imediata a partir do Teorema, uma vez que em qualquer um dos

casos temos

$$[K_2 : K_1]_s = 1.$$

■

Teorema 3.5.29 *Suponhamos que K é um corpo separavelmente fechado e $\mathcal{O}$ é um anel de valorização próprio de K. Seja $\widetilde{K}$ um fecho algébrico de K e $\widetilde{\mathcal{O}}$ a única extensão de $\mathcal{O}$ para $\widetilde{K}$. Então:*

i) $\widetilde{\mathcal{O}}/\mathcal{O}$ é uma extensão imediata.

ii) O corpo de resíduos $\overline{K}$ de $\mathcal{O}$ é algebricamente fechado.

iii) O grupo de valores Γ de $\mathcal{O}$ é divisível.

Prova. Inicialmente observamos que, sendo K separavelmente fechado, temos $\widetilde{K}|K$ uma extensão puramente inseparável. Portanto, pelo Corolário 3.5.28, temos de fato que $\widetilde{\mathcal{O}}$ é a única extensão de $\mathcal{O}$ para $\widetilde{K}$.

Denotemos por $\widetilde{\Gamma}$ e $\overline{\widetilde{K}}$ o grupo e o corpo de resíduos de $\widetilde{\mathcal{O}}$, respectivamente. Então, pelo Lema 3.4.4, $\widetilde{\Gamma}$ é um grupo divisível e $\overline{\widetilde{K}}$ é um corpo algebricamente fechado.

Provemos que $\overline{K} = \overline{\widetilde{K}}$. Dado $x \in \widetilde{\mathcal{O}}^{\times}$, como $\overline{\widetilde{K}}|\overline{K}$ é uma extensão algébrica (veja Corolário 3.5.11), existe um polinômio mônico

$$g(X) = a_0 + a_1X + ... + a_{n-1}X^{n-1} + X^n \in \mathcal{O}[X]$$

tal que $\overline{g}$ é o polinômio minimal de $\overline{x} \in \overline{\widetilde{K}}$ sobre $\overline{K}$.

Pelo Lema 3.4.19 encontramos um polinômio mônico separável e de mesmo grau que g,

$$h(X) = b_0 + b_1X + ... + b_{n-1}X^{n-1} + X^n \in K[X]$$

satisfazendo

$$v(a_i - b_i) > 0,$$

para todo $i \in \{0, ..., n\}$, onde v denota a valorização de K associada a $\mathcal{O}$. Como $g \in \mathcal{O}[X]$, temos também

$$h \in \mathcal{O}[X]$$

e, para todo $i \in \{0, ..., n\}$,

$$\overline{a_i} = \overline{b_i} \tag{34}$$

em $\overline{K}$.

Sendo $h \in K[X]$ separável e K separavelmente fechado, temos que todas as raízes de h pertencem a K, e mais até: como $\mathcal{O}$ integralmente fechado em K, e $h \in \mathcal{O}[X]$ é mônico, pelo Teorema 3.4.12(1) temos que $z \in \mathcal{O}$, para toda raiz z de h, e portanto podemos falar do elemento $\overline{z} \in \overline{K}$. Em $\overline{K}$,

$$\overline{g}(\overline{z}) \overset{(34)}{=} \overline{h} = \overline{h(z)} = \overline{0}.$$

Assim, $\overline{g}$, que é o polinômio minimal de $\overline{x}$ sobre $\overline{K}$, tem uma raiz em $\overline{z} \in \overline{K}$. Então $\overline{g}$ tem grau 1 e $\overline{x} = \overline{z} \in \overline{K}$ como queríamos provar.

Provemos agora que $\Gamma = \widetilde{\Gamma}$. Dado $\delta \in \widetilde{\Gamma}$, o Teorema 3.5.18 nos garante a existência de $n > 1$ e $a \in K$ tais que

$$n\delta = v(a) \in \Gamma,$$

onde v é a valorização de K correspondente ao anel de valorização $\mathcal{O}$. Sem perda de generalidade tomamos $\delta > 0$, e então $a \in \mathcal{O}$.

Seja

$$g(X) = X^n - a.$$

Então, pelo Lema 3.4.19, podemos aproximar $g(X)$ por um polinômio separável $h(X) = b_0 + b_1 X + ... + X^n \in K[X]$ satisfazendo

$$v(a_i - b_i) > n\delta,$$

para todo $0 \leq i \leq n$. Como K é separavelmente fechado e $\mathcal{O}$ é integralmente fechado em K, o polinômio h tem uma raiz $z \in \mathcal{O}$, e portanto faz sentido calcularmos $v(g(z))$:

$$v(g(z)) \overset{h(z)=0}{=} v(g(z) - h(z)) \geq \min_{0 \leq i \leq n} \{v(a_i - b_i) + iv(z)\} > n\delta = v(a).$$

Porém

$$v(z^n - a) = v(g(z)) > v(a)$$

implica

$$v(z^n) = v(a) = n\delta,$$

e então

$$nv(z) = n\delta.$$

Como todo grupo abeliano totalmente ordenado é livre de torção, concluímos:

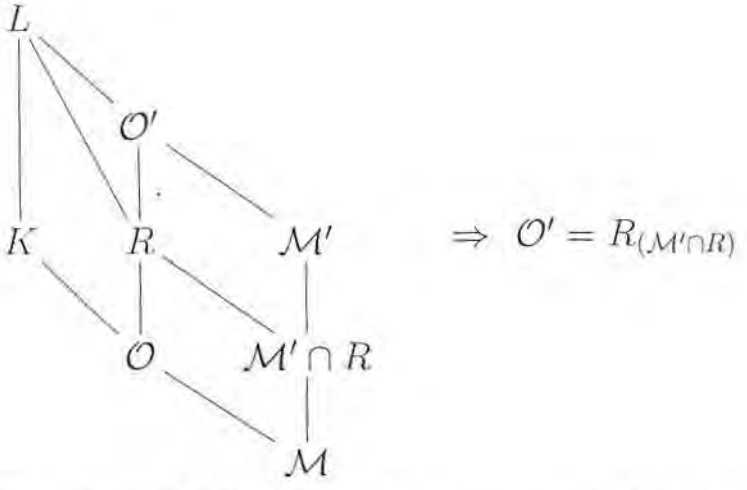
$$\delta = v(z) \in \Gamma.$$

■

No próximo resultado, mostramos que o fecho inteiro de um anel de valorização de K em uma extensão algébrica de K tem uma propriedade semelhante àquela vista no Lema 3.4.13 quando tratávamos de um só corpo.

Teorema 3.5.30 *Sejam L uma extensão algébrica do corpo K e $\mathcal{O}$ um anel de valorização de K. Denotamos por R o fecho inteiro de $\mathcal{O}$ em L. Tome $\mathcal{O}'$ uma extensão de $\mathcal{O}$ em L. Se $\mathcal{M}'$ é o ideal maximal de $\mathcal{O}'$ e $m = \mathcal{M}' \cap R$ então*

$$R_m = \mathcal{O}'.$$



Prova. Pelo Corolário 3.5.5, R é a intersecção de todos os anéis de valorização de L que prolongam $\mathcal{O}$. Assim, é claro que $R \subseteq \mathcal{O}'$, e como

$m = \mathcal{M}' \cap R$, temos também

$$R_m \subseteq \mathcal{O}'.$$

Para provar a recíproca, consideramos $x \in \mathcal{O}'$ e o corpo intermediário $K_2 = K(x)$ e definimos

$$\begin{aligned} R_2 &:= R \cap K_2, \\ m_2 &:= m \cap K_2 = \mathcal{M}' \cap R \cap K_2 = \mathcal{M}', \\ \mathcal{O}_2 &:= \mathcal{O}' \cap K_2, \\ \mathcal{M}_2 &:= \mathcal{M}' \cap K_2. \end{aligned}$$

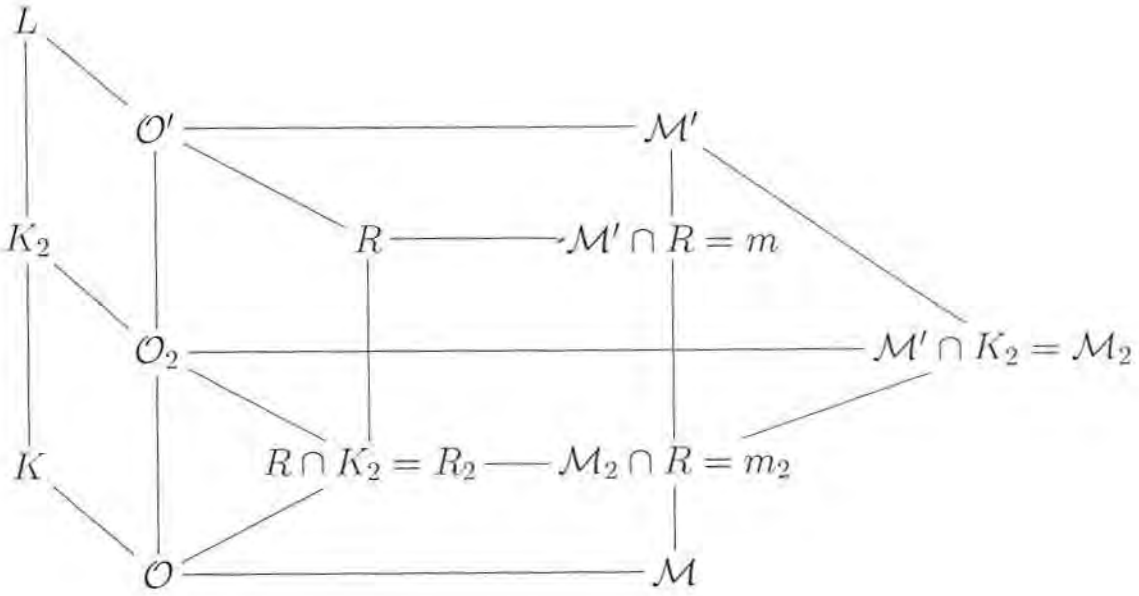
Obviamente

$$R_2 = R \cap K_2 \subset \mathcal{O}' \cap K_2 = \mathcal{O}_2, \ \mathcal{M}_2 = \mathcal{M}' \cap K_2 \subset \mathcal{O}' \cap K_2 = \mathcal{O}_2,$$

e

$$m \cap \mathcal{O}_2 = \mathcal{M}' \cap R \cap \mathcal{O}_2 = \mathcal{M}' \cap R \cap \mathcal{O}' \cap K_2 = \mathcal{M}' \cap K_2 \cap R = \mathcal{M}_2 \cap R.$$

As igualdades acima nos permitem construir o seguinte diagrama



Claramente R_2 é o fecho inteiro de $\mathcal{O}$ em K_2, e pelo Corolário 3.5.5

$$R_2 = \bigcap \mathcal{O}^*,$$

onde $\mathcal{O}^*$ varia no conjunto de todos os prolongamentos de $\mathcal{O}$ em K_2.

Pelo Teorema 3.5.27 o anel $\mathcal{O}$ tem somente um número finito de extensões em K_2, uma vez que

$$[K_2 : K]_s \leq [K_2 : K] < \infty.$$

Assim, o Lema 3.4.13 pode ser aplicado: como $\mathcal{M}_2 \cap R_2 = m_2$, temos

$$\mathcal{O}_2 = (R_2)_{m_2}.$$

Portanto, como $x \in \mathcal{O}' \cap K_2 = \mathcal{O}_2$, existem $a, b \in R_2$ com $b \notin m_2$ tais que $x = a/b$. Mas então $R_2 = R \cap K_2$ e

$$m_2 = m_2 \cap R_2 = \mathcal{M}' \cap K_2 \cap R \cap R_2 = \mathcal{M}' \cap R \cap K_2 = m \cap K_2,$$

de modo que $b \in K_2$ mas $b \notin m \cap K_2$, o que nos dá $b \notin m$. Assim, podemos também dizer que $a, b \in R$ e $b \notin m$ e portanto

$$x = \frac{a}{b} \in R_m.$$

■

Analisamos agora o conjunto de todos os prolongamentos de um anel de valorização de K a uma extensão normal de K. Começamos com as extensões finitas:

Teorema 3.5.31 *Sejam $L|K$ uma extensão finita e normal de corpos e $G = Aut(L|K)$ o grupo de $K-$automorfismos de L. Sejam $\mathcal{O}$ um anel de valorização de K e $\mathcal{O}'$, $\mathcal{O}''$ anéis de valorização de L que estendem $\mathcal{O}$. Então $\mathcal{O}'$ e $\mathcal{O}''$ são $K-$conjugados, ou seja, existe $\sigma \in G$ com $\sigma(\mathcal{O}') = \mathcal{O}''$.*

Prova. Inicialmente afirmamos que basta considerarmos o caso em que $L|K$ é separável. De fato, considerando o corpo intermediário $L \cap K^s$, isto

é,

$$K \subset L \cap K^s \subset L,$$

temos $L|(L \cap K^s)$ puramente inseparável, e pelo Corolário 3.5.28 toda extensão de $\mathcal{O}$ em $L \cap K^s$ tem apenas um prolongamento a L. Além disto, $Aut(L \cap K^s|K)$ e G podem ser canonicamente identificados.

Suponhamos então que $L|K$ é separável. Neste caso, consideramos os seguintes subgrupos de G:

$$H' = \{\sigma \in G \mid \sigma(\mathcal{O}') = \mathcal{O}'\} \quad \text{e} \quad H'' = \{\tau \in G \mid \tau(\mathcal{O}'') = \mathcal{O}''\}.$$

Para todo $\sigma \in H'$ temos

$$\sigma(\mathcal{M}') = \mathcal{M}', \tag{35}$$

onde $\mathcal{M}'$ é o ideal maximal de $\mathcal{O}'$. Para isto basta observar que, sendo σ um automorfismo, $\sigma(\mathcal{M}')$ deve ser o ideal maximal de $\sigma(\mathcal{O}') = \mathcal{O}'$. Analogamente,

$$\tau(\mathcal{M}'') = \mathcal{M}''$$

para todo $\tau \in H''$.

Escrevemos G como uma união disjunta de classes laterais com respeito a H' e H'' da seguinte forma

$$G = \bigcup_{i=1}^{n} H'\sigma_i^{-1} \quad \text{e} \quad G = \bigcup_{j=1}^{m} H''\tau_j^{-1},$$

para certos $\sigma_i, \tau_j \in G$. Estas partições são cruciais para o estudo do conjunto de todas as extensões de $\mathcal{O}$ em L.

Afirmamos que existem $i \in \{1, ..., n\}$ e $j \in \{1, ..., m\}$ tais que $\sigma_i(\mathcal{O}') = \tau_j(\mathcal{O}'')$ e portanto

$$\mathcal{O}'' = \tau_j^{-1}\sigma_i(\mathcal{O}'),$$

o que completa a prova.

Suponhamos o contrário, isto é, que, para quaisquer $i \in \{1, ..., n\}$ e

$j \in \{1, ..., m\}$,

$$\sigma_i(\mathcal{O}') \nsubseteq \tau_j(\mathcal{O}'') \quad \text{e} \quad \tau_j(\mathcal{O}'') \nsubseteq \sigma_i(\mathcal{O}'),$$

Sabido que $\{\sigma_1^{-1}, ..., \sigma_n^{-1}\}$ é um conjunto completo de representantes das classes laterais de H', temos

$$\sigma_k(\mathcal{O}') \nsubseteq \sigma_t(\mathcal{O}'),$$

sempre que $k \neq t$, com $1 \leq k, t \leq n$, pois

$$\sigma_k(\mathcal{O}') \subseteq \sigma_t(\mathcal{O}') \overset{\text{Lema 3.5.22}}{\Rightarrow} \sigma_k(\mathcal{O}') = \sigma_t(\mathcal{O}'),$$

uma vez que são ambos anéis de valorização que prolongam $\mathcal{O}$; assim, $\sigma_t^{-1}\sigma_k \in H'$ e portanto

$$\sigma_t H' = \sigma_k H',$$

o que nos permite também concluir que $k = t$.

Por raciocínio análogo, concluímos que

$$\tau_k(\mathcal{O}'') \nsubseteq \tau_l(\mathcal{O}''),$$

para todo $k \neq t$ com $1 \leq k, t \leq m$.

Seja

$$R := \bigcap_{i=1}^{n} \sigma_i(\mathcal{O}') \quad \cap \quad \bigcap_{j=1}^{m} \tau_j(\mathcal{O}'').$$

Pelo Teorema 3.4.14 (3) existe $a \in R$ tal que

$$a-1 \in \sigma_i(\mathcal{M}') \text{ para todo } 1 \leq i \leq n \quad \text{e} \quad a \in \tau_j(\mathcal{M}'') \text{ para todo } 1 \leq j \leq m. \tag{36}$$

Dado $\sigma \in G$, digamos,

$$\sigma = \rho\sigma_i^{-1},$$

para algum $i \in \{1, ..., n\}$ e $\rho \in H'$, segue de (36) que

$$\sigma(a-1) \in \rho\sigma_i^{-1}(\sigma_i(\mathcal{M}')) = \rho(\mathcal{M}') \overset{(35)}{=} \mathcal{M}',$$

para todo $\sigma \in G$. Analogamente, também

$$\sigma(a) \in \mathcal{M}''.$$

Considerando a norma $\mathcal{N}_{L|K}$ da extensão $L|K$, temos então

$$x := \mathcal{N}_{L|K}(a) = \prod_{\sigma \in G} \sigma(a) \in (1 + \mathcal{M}') \cap K = 1 + \mathcal{M}$$

mas também

$$x = \mathcal{N}_{L/K}(a) = \prod_{\sigma \in G} \sigma(a) \in \mathcal{M}'' \cap K = \mathcal{M}.$$

Isto significa $v(x) = 0$ e $v(x) > 0$, um absurdo.

Esta contradição implica que existem i e j com $\sigma_i(\mathcal{O}') \subseteq \tau_j(\mathcal{O}'')$ ou $\tau_j(\mathcal{O}'') \subseteq \sigma_i(\mathcal{O}')$. Novamente, pelo Lema 3.5.22 temos

$$\sigma_i(\mathcal{O}') = \tau_j(\mathcal{O}'').$$

■

O resultado acima se generaliza para extensões normais arbitrárias:

Teorema 3.5.32 (Teorema da Conjugação) *Seja $L|K$ uma extensão normal arbitrária de corpos. Se $\mathcal{O}$ é um anel de valorização de K e $\mathcal{O}'$ e $\mathcal{O}''$ são anéis de valorização de L que estendem $\mathcal{O}$ então existe $\sigma \in Aut(L|K)$ tal que*

$$\sigma(\mathcal{O}') = \mathcal{O}''.$$

Prova. Consideramos o conjunto $\mathcal{F}$ dos pares ordenados (K_1, σ_1) onde K_1 é um corpo intermediário tal que $K_1|K$ é normal e σ_1 é um automorfismo da extensão $K_1|K$ com

$$\sigma_1(\mathcal{O}_1') = \mathcal{O}_1'',$$

onde

$$\mathcal{O}_1' = \mathcal{O}' \cap K_1 \quad \text{e} \quad \mathcal{O}_1'' = \mathcal{O}'' \cap K_1.$$

Claramente (K, id_K) está neste conjunto. Definimos em $\mathcal{F}$ uma ordem parcial:

$$(K_1, \sigma_1) \leq (K_2, \sigma_2) : \Leftrightarrow \ K_1 \subseteq K_2 \text{ e } \sigma_1 = \sigma_2|_{K_1}.$$

É fácil convencer-se que todo subconjunto totalmente ordenado de $\mathcal{F}$ possui uma cota superior.

Assim, o Lema de Zorn pode ser aplicado ao conjunto $\mathcal{F}$, e então existe um par maximal (K^*, σ^*):

$$K \subseteq K^* \subseteq L \quad \text{e} \quad \sigma^*(\mathcal{O}'_*) = \mathcal{O}''_*,$$

onde

$$\mathcal{O}'_* := \mathcal{O}' \cap K^* \quad \text{e} \quad \mathcal{O}''_* := \mathcal{O}'' \cap K^*.$$

Afirmamos que $K^* = L$. De fato, caso contrário existe

$$\alpha \in L \backslash K^*.$$

Sejam f o polinômio minimal de α com respeito a K e N o corpo de decomposição de f sobre K^* em L. Estendemos σ^* a um automorfismo do fecho algébrico $\widetilde{K}$ de K, e continuamos a denotá-lo por σ^*.

Temos então

$$\sigma^*(L) = L \quad \text{e} \quad \sigma^*(N) = N.$$

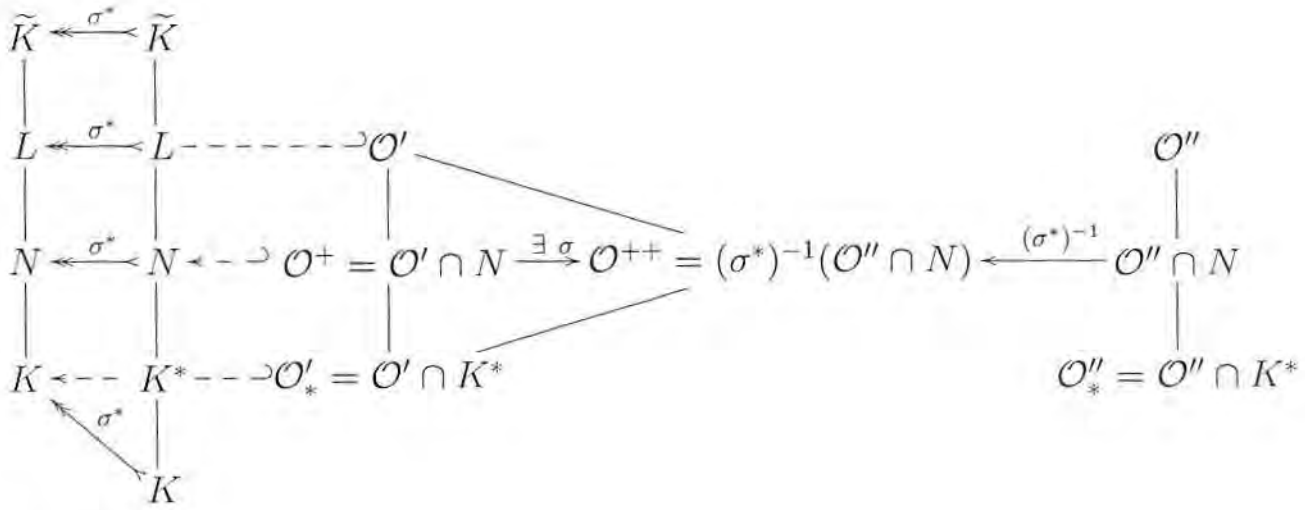
De fato, $L|K$ é uma extensão normal por hipótese; além disso, N é o compositum de K^* com o corpo de decomposição de α sobre K em L.

Sejam

$$\mathcal{O}^+ := \mathcal{O}' \cap N \quad \text{e} \quad \mathcal{O}^{++} := (\sigma^*)^{-1}(\mathcal{O}'' \cap N).$$

Seguindo o diagrama abaixo afirmamos que

$$\mathcal{O}^+ \cap K^* = \mathcal{O}^{++} \cap K^* = \mathcal{O}'_*.$$



De fato, como

$$\sigma_*(\mathcal{O}'_*) = \mathcal{O}''_*,$$

temos

$$\sigma_*^{-1}(\mathcal{O}''_*) = \mathcal{O}'_*,$$

o que implica

$$\mathcal{O}^+ \cap K^* = \mathcal{O}^{++} \cap K^* = \mathcal{O}'_*.$$

Aplicando o Teorema 3.5.31 aos anéis $\mathcal{O}^+$ e $\mathcal{O}^{++}$ obtemos $\tau \in Aut(N/K^*)$ com $\mathcal{O}^{++} = \tau(\mathcal{O}^+)$. Então

$$\sigma^* \circ \tau(\mathcal{O}' \cap N) = \sigma^* \circ \tau(\mathcal{O}^+) = \sigma^*(\mathcal{O}^{++}) = \sigma^*(\sigma^*)^{-1}(\mathcal{O}'' \cap N) = \mathcal{O}'' \cap N.$$

Portanto

$$(K^*, \sigma^*) < (N, \sigma^* \circ \tau),$$

contradizendo a maximalidade de (K^*, σ^*).

■

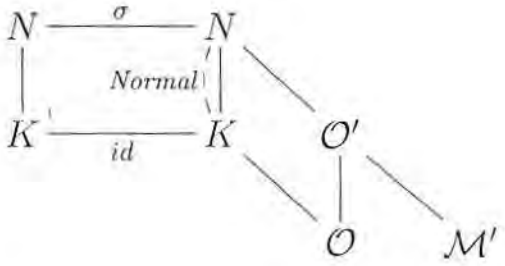
Continuamos a listar propriedades de extensões normais que nos serão úteis.

Proposição 3.5.33 *Sejam $N|K$ uma extensão normal, $\mathcal{O}$ um anel de valorização de K, $\mathcal{O}'$ anel de valorização de N que estende $\mathcal{O}$ e $\mathcal{M}'$ o ideal*

maximal de $\mathcal{O}'$. Sejam

$$v : K \twoheadrightarrow \Gamma \cup \{\infty\},$$

$$v' : N \twoheadrightarrow \Gamma' \cup \{\infty\},$$



as valorizações associadas a $\mathcal{O}$ e $\mathcal{O}'$ respectivamente tais que $v = v'|_K$, isto é, $\Gamma \subset \Gamma'$

Denotando o corpo de resíduos de $\mathcal{O}'$ e $\mathcal{O}$ por $\overline{N}$ e $\overline{K}$ respectivamente, temos:

(1) *Dado $\sigma \in Aut(N|K)$ a aplicação $v' \circ \sigma : N \twoheadrightarrow \Gamma' \cup \{\infty\}$ é a única valorização de N correspondente ao anel de valorização $\sigma^{-1}(\mathcal{O}')$ com grupo de valores Γ'. Em particular,*

$$\sigma(\mathcal{O}') = \mathcal{O}' \Rightarrow v' \circ \sigma = v'.$$

(2) *$\overline{N}|\overline{K}$ é uma extensão normal.*

(3) *A aplicação $x \mapsto \overline{\sigma(x)}$ define um homomorfismo de anéis*

$$\varphi : \sigma^{-1}(\mathcal{O}') \twoheadrightarrow \overline{N}$$

que, por sua vez, induz um $\overline{K}$-isomorfismo

$$\varphi' : \sigma^{-1}(\mathcal{O}')/\sigma^{-1}(\mathcal{M}') \twoheadrightarrow \overline{N},$$

o qual também satisfaz

$$\overline{\sigma}(u + \sigma^{-1}(\mathcal{M}')) = \overline{\sigma(u)},$$

para todo $u \in \sigma^{-1}(\mathcal{O}')$. *Em particular,*

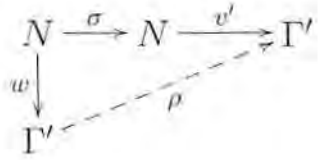
$$\sigma(\mathcal{O}') = \mathcal{O}' \Rightarrow \overline{\sigma} \in Aut(\overline{N}|\overline{K}).$$

(4) *Para todo* $\sigma \in Aut(N|K)$,

$$e(\sigma^{-1}(\mathcal{O}')/\mathcal{O}) = e(\mathcal{O}'/\mathcal{O}) \quad e \quad f(\sigma^{-1}(\mathcal{O}')/\mathcal{O}) = f(\mathcal{O}'/\mathcal{O}).$$

Prova. (1) É claro que

$$k \longmapsto k \longmapsto \gamma \in \Gamma$$



com

$$w := v' \circ \sigma : N \twoheadrightarrow \Gamma' \cup \{\infty\}$$

é uma valorização de N; além disso, o anel de valorização associado a $v' \circ \sigma$ é

$$\{x \in N \mid (v' \circ \sigma)(x) \geq 0\} = \{x \in N \mid \sigma(x) \in \mathcal{O}'\} = \sigma^{-1}(\mathcal{O}').$$

Seja

$$w : N \twoheadrightarrow \Gamma' \cup \{\infty\}$$

uma valorização em N cujo anel de valorização é $\sigma^{-1}(\mathcal{O}')$. Então $v' \circ \sigma$ e w são valorizações equivalentes. Pela Proposição 3.3.26 existe um isomorfismo que preserva a ordem

$$\rho : \Gamma' \to \Gamma'$$

tal que

$$\rho \circ w = v' \circ \sigma.$$

Logo $\rho(\gamma) = \gamma$ para todo $\gamma \in \Gamma$.

E, para $\gamma \in \Gamma'$, pelo Teorema 3.5.18, existe $n > 1$ tal que $n\gamma \in \Gamma$.

Portanto

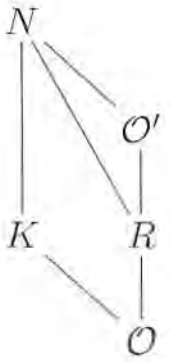
$$n\rho(\delta) = \rho(n\delta) = n\delta,$$

o que implica $\rho(\delta) = \delta$, pois Γ' como grupo de valores é livre de torção. Ou seja,

$$\rho = id_{\Gamma'} \quad \text{e} \quad w = v' \circ \sigma,$$

o que completa a prova.

(2) Inicialmente consideramos o fecho inteiro de $\mathcal{O}$ em N, que vamos denotar por R. Sabemos que $R \subset \mathcal{O}'$.



Escrevendo

$$m = \mathcal{M}' \cap R,$$

temos, pelo Teorema 3.5.30, que

$$\mathcal{O}' = R_m.$$

Assim, a aplicação

$$R_m = \mathcal{O}' \to \mathcal{O}'/\mathcal{M}'$$

$$x \mapsto \overline{x} = x + \mathcal{M}'$$

induz uma aplicação sobrejetora

$$R \twoheadrightarrow \overline{N} = \frac{\mathcal{O}'}{\mathcal{M}'}, \tag{37}$$

pois

$$\overline{N} = \frac{\mathcal{O}'}{\mathcal{M}'} = \frac{R_m}{mR_m} \simeq \frac{R}{m}.$$

Afirmamos ainda que, para todo $\sigma \in Aut(N|K)$, temos

$$\sigma(R) = R.$$

De fato, cada σ permuta os anéis de valorização de N que estendem $\mathcal{O}$. Portanto, para $x \in R$ temos

$$\sigma(x) \in R \tag{38}$$

para todo $\sigma \in Aut(N|K)$. Para a recíproca, basta lembrar que, dado $x \in R$ e para todo $\tau \in Aut(N|K)$, $\tau^{-1}(x) \in R$ e portanto

$$x = \sigma(\sigma^{-1}(x)) \in \sigma(R).$$

Já sabemos, pelo Teorema 3.5.18, que $\overline{N}|\overline{K}$ é uma extensão algébrica. Para mostrar que ela é até normal, consideramos $\alpha \in \overline{N}$ e denotamos por $\overline{f} \in \overline{K}[X]$ o polinômio minimal de α sobre $\overline{K}$. Por (37), existe $x \in R$ tal que

$$\overline{x} = \alpha.$$

Como $x \in R \subset N$, temos que x é algébrico sobre K. Seja $g \in K[X]$ o polinômio minimal de x sobre K. Como $N|K$ é normal e $x \in N$,

$$g = (X - x_1)...(X - x_n),$$

onde $n = \deg(g)$ e $x = x_1, ..., x_n$ são conjugados de x. Portanto, por (38), $x = x_1, ..., x_n \in R \subset \mathcal{O}'$ e então $g(X) \in \mathcal{O}'[X]$.

Assim, faz sentido considerarmos $\overline{g}(X)$. Daí,

$$\overline{g}(\alpha) = \overline{g}(\overline{x}) = \overline{g(x)} = \overline{0},$$

e portanto temos que $\overline{f}$ divide $\overline{g}$. Mas

$$\overline{g} = (X - \overline{x_1})...(X - \overline{x_n})$$

em $\overline{N}$. Portanto $\overline{f}$ também se fatora completamente em $\overline{N}$, o que prova

(2).

(3) A aplicação $x \mapsto \overline{\sigma(x)}$ pode ser vista como um homomorfismo de anéis, logo é um homomorfismo de anéis. A outra afirmação é provada fazendo computações usuais.

(4) É uma consequência imediata de (1) e (3).

■

Observação 3.5.34 *Seja $L|K$ uma extensão de Galois finita de grau n, e suponhamos que um anel de valorização $\mathcal{O}$ de K tem um único prolongamento $\mathcal{O}'$ a L. Seja v a valorização sobre K correspondente a $\mathcal{O}$. Então,*

$$w \circ \sigma = w,$$

para cada $\sigma \in Aut(L|K)$, onde w é o único prolongamento de v a L. Daí, para cada $x \in \mathcal{O}'$, denotando por $\mathcal{N}_{L|K} : L \to K$ a aplicação norma da extensão, temos

$$\begin{aligned}
\mathcal{N}_{L|K}(x) \in K \Rightarrow v(\mathcal{N}_{L|K}(x)) &= w(\mathcal{N}_{L|K}(x)) \\
&= w\left(\prod_{\sigma \in Aut(L|K)} \sigma(x)\right) \\
&= \sum_{\sigma \in Aut(L|K)} (w \circ \sigma)(x) \\
&= \sum_{\sigma \in Aut(L|K)} w(x) = nw(x),
\end{aligned}$$

e portanto

$$w(x) = \frac{1}{n}\, v(\mathcal{N}_{L|K}(x)).$$

Na verdade podemos retirar a hipótese de finitude no seguinte sentido: no caso de L ser o fecho separável de K, dado $x \in L$ seja

$$f(X) = a_0 + a_1 X + ... + X^n$$

o seu polinômio minimal sobre K. Então

$$w(x) = \frac{1}{n}\, v(a_0).$$

De fato, sejam $x = x_1, ..., x_n$ todos os conjugados de x. Então $w(x) = w(x_i)$ pela parte (1). Portanto

$$v(\mathcal{N}(x)) = w(x_1 x_2 ... x_n) = nw(x).$$

3.6 Corpos Valorizados Henselianos

Nesta seção vamos estudar uma classe muito importante de corpos valorizados, os *corpos henselianos*. Eles ganham este nome pelo fato de tais corpos satisfazerem o Lema de Hensel, em sua versão mais geral do que aquela apresentada no Teorema 3.2.13. Mais precisamente, os corpos henselianos são até caracterizados pela validade deste Lema.

Tentando abordar questões de irredutibilidade de polinômios sobre corpos valorizados, chega-se ao conceito de corpo valorizado henseliano. Apresentamos aqui a relação entre irredutibillidade de polinômios e corpos henselianos (veja Teorema 3.6.4(3)).

Mostramos ainda que todo corpo valorizado admite uma extensão algébrica maximal única, a menos de isomorfismos, que estendem também a valorização e que satisfaz o Lema de Hensel. Esta extensão será chamada de *henselização do corpo valorizado* originalmente dado.

As referências para esta seção são [3] e [4]. Também em [12] podemos encontrar mais detalhes sobre a teoria de corpos henselianos.

Para a prova da versão geral do Lema de Hensel, é útil introduzirmos antes uma nomenclatura.

Definição 3.6.1 *Dizemos que um polinômio $f \in K[X]$ primitivo (com respeito à valorização w) caso $w(f) = 0$, onde w é a valorização de Gauss que estende uma valorização v em K.*

Relembramos que a cada valorização

$$v : K \twoheadrightarrow \Gamma \cup \{\infty\}$$

de K está associada a valorização de Gauss, que é a valorização de $K(X)$ que estende v e que é induzida por

$$w(f) = \min_{0 \leq i \leq n} v(a_i).$$

se $f = a_0 + a_1 X + ... + a_n X^n \in K[X]$. (veja Corolário 3.5.14)

Valem as seguintes propriedades sobre polinômios primitivos:

Lema 3.6.2 (Lema de Gauss para corpos valorizados) *Sejam $(K, \mathcal{O})$ um corpo valorizado e v a correspondente valorização*

(1) *Se $f \in K[X]$ é primitivo então $f \in \mathcal{O}[X]$.*

(2) *Se dois polinômios $f, g \in K[X]$ são primitivos então o produto $f.g$ também o é.*

(3) *Todo $f \in K[X]$ admite uma decomposição $f = af_1$ com $a \in K$ e $f_1 \in \mathcal{O}[X]$ sendo primitivo.*

(4) *Se $f \in \mathcal{O}[X]$ se fatora como*

$$f = g_1 ... g_m$$

com fatores irredutíveis $g_1, ..., g_m \in K[X]$ então existem $h_1, ..., h_m \in \mathcal{O}[X]$, irredutíveis em $K[X]$, tais que

$$f = h_1 ... h_m.$$

Mais ainda, se f é primitivo então $h_1, ..., h_m$ também o são.

Prova. A propriedade (1) é claramente verdadeira. Para convencer-se de (2), basta lembrar que

$$w(fg) = w(f) + w(g).$$

Agora, se $f \in K[X]\backslash\{0\}$ e

$$f = a_n X^n + ... + a_0,$$

então, escolhendo $i \in \{1, ..., n\}$ tal que

$$v(a_i) = \min_{1 \leq j \leq n} \{v(a_j)\} = w(f),$$

temos que

$$f = a_i \underbrace{\left(\frac{a_n}{a_i} X^n + ... + \frac{a_0}{a_i} \right)}_{=: f_1},$$

e claramente $w(f_1) = 0$, o que prova (3).

Para verificar (4) dada a fatoração

$$f = g_1 ... g_m,$$

escrevemos, utilizando (3),

$$g_i = b_i \widetilde{g_i},$$

para cada $i \in \{1, ..., m\}$, com $b_1, ..., b_m \in K$ e $\widetilde{g_1}, ..., \widetilde{g_m}$ primitivos. Com isto, para cada $i \in \{1, ..., m\}$,

$$w(g_i) = w(b_i \widetilde{g_i}) = w(b_i) + w(\widetilde{g_i}) = w(b_i) = v(b_i).$$

Então

$$v(b_1 ... b_m) = \sum_{i=1}^{m} v(b_i) = \sum_{i=1}^{m} w(g_i) = w(f) \overset{f \in \mathcal{O}[X]}{\geq} 0.$$

Portanto, tomando

$$b = b_1 ... b_m \in \mathcal{O}$$

e definindo

$$h_1 = b\widetilde{g_1} \in \mathcal{O}[X] \quad \text{e} \quad h_i = \widetilde{g_i} \in \mathcal{O}[X],$$

para cada $i \in \{2, ..., m\}$, obtemos a decomposição desejada.

Claramente, se f é primitivo então $v(b) = 0$ e a última afirmação segue.

■

A condição (4) acima nos diz que, para verificarmos se um polinômio $f \in \mathcal{O}[X]$ é irredutível em $K[X]$, basta provarmos que ele não possui fatoração não trivial em $\mathcal{O}[X]$.

Dado um corpo valorizado $(K, \mathcal{O})$ e $f \in \mathcal{O}[X]$ mônico (portanto primitivo) satisfazendo $\deg(f) > 0$, se f admitir uma fatoração não trivial em $\mathcal{O}[X]$, digamos,

$$f = g_1 g_2, \text{ com } g_1, g_2 \in \mathcal{O}[X] \text{ mônicos (portanto primitivos)}$$

com

$$\deg(g_1) > 0 \text{ e } \deg(g_2) > 0,$$

então $\overline{f}$ tem também uma fatoração não trivial em $\overline{K}[X]$:

$$\overline{f} = \overline{g_1}.\overline{g_2}, \text{ com } \deg(g_1) > 0 \text{ e } \deg(g_2) > 0.$$

Note que por serem primitivos, eles não se anulam em $\overline{K}[X]$.

Assim, se f é redutível, então $\overline{f}$ também o é. No entanto, a recíproca não é verdadeira, como nos mostra o seguinte exemplo:

Exemplo 3.6.3 *Para cada primo p, o polinômio $f = X^2 + (2p+1)X + p \in \mathbb{Q}[X]$ é irredutível em $\mathbb{Z}_{p\mathbb{Z}}[X]$, mas em $\overline{\mathbb{Q}} = \mathbb{F}_p$,*

$$\overline{f} = X^2 + X = X(X + \overline{1}),$$

e X e $X + \overline{1}$ mônicos em $\mathbb{F}_p[X]$.

Hensel considerou os corpos valorizados para os quais a situação acima não ocorre. (veja (3) no Teorema abaixo.)

Vamos agora provar uma série de equivalências que vão originar a definição de corpo valorizado henseliano, sendo por isso chamada de "Lema de Hensel".

Teorema 3.6.4 (Lema de Hensel geral) *Dado um corpo valorizado $(K, \mathcal{O})$, sejam $\mathcal{M}, \overline{K}$ e $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ o ideal maximal, o corpo de*

resíduos e a valorização correspondentes a $\mathcal{O}$, respectivamente. Definimos também a aplicação $a \mapsto \overline{a}$, o homomorfismo residual, e a aplicação $f \mapsto \overline{f}$ de $\mathcal{O}[X]$ em $\overline{K}[X]$ que o estende a $\overline{K}[X]$. As seguintes afirmações são equivalentes:

(1) *Para toda extensão algébrica $L|K$, o anel de valorização $\mathcal{O}$ tem uma única extensão a L.*

(2) *Para cada polinômio irredutível $f \in \mathcal{O}[X]$ com $\overline{f} \notin \overline{K}$, existem $g \in \mathcal{O}[X]$ e $a \in \mathcal{O}$ com $\overline{g}$ irredutível em $\overline{K}[X]$ e $\overline{a} \neq \overline{0}$ em $\overline{K}$, tais que $\overline{f} = \overline{a}\ \overline{g}^{\,s}$, para algum $s \geq 1$.*

(3) *Sejam $f, g, h \in \mathcal{O}[X]$ satisfazendo $\overline{f} = \overline{g}.\overline{h}$ com $\overline{g}$ e $\overline{h}$ relativamente primos em $\overline{K}[X]$. Então existem $g_1, h_1 \in \mathcal{O}[X]$ com $f = g_1.h_1$, $\overline{g_1} = \overline{g}$, $\overline{h_1} = \overline{h}$ e $\deg(g_1) = \deg(\overline{g})$.*

(4) *Para cada $f \in \mathcal{O}[X]$ e $a \in \mathcal{O}$ com $\overline{f}(\overline{a}) = 0$ e $\overline{f}\,'(\overline{a}) \neq 0$,[5] existe $\alpha \in \mathcal{O}$ com $f(\alpha) = 0$ e $\overline{\alpha} = \overline{a}$.*

(5) *Para cada $f \in \mathcal{O}[X]$ e $a \in \mathcal{O}$ com $v(f(a)) > 2v(f'(a))$, existe um $\alpha \in \mathcal{O}$ com $f(\alpha) = 0$ e $v(a - \alpha) > v(f'(a))$.*

(6) *Todo polinômio $X^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathcal{O}[X]$ com $a_{n-1} \notin \mathcal{M}$ e $a_{n-2}, ..., a_0 \in \mathcal{M}$ tem um zero em $\mathcal{O}$.*

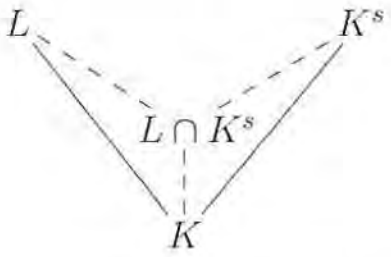
(7) *Todo polinômio $X^n + X^{n-1} + a_{n-2}X^{n-2} + ... + a_0 \in \mathcal{O}[X]$ com $a_{n-2}, ..., a_0 \in \mathcal{M}$ tem um zero em $\mathcal{O}$.*

(8) *O anel de valorização $\mathcal{O}$ tem uma única extensão a K^s.*

Prova. (1) $\Leftrightarrow$ (8): Suponhamos que para toda extensão algébrica $L|K$ existe uma única extensão de $\mathcal{O}$ a L. Então, em particular, $\mathcal{O}$ estende-se unicamente para a extensão algébrica K^s.

[5] Em particular isto ocorre se $\overline{f}$ é separável.

Para provar a recíproca, consideramos uma extensão algébrica $L|K$.



Toda extensão $\mathcal{O}'$ de $\mathcal{O}$ a $L \cap K^s$ tem uma extensão $\mathcal{O}^s$ a K^s que também estende $\mathcal{O}$. Por hipótese ela é única, e portanto a extensão $\mathcal{O}'$ de $\mathcal{O}$ também é única. Pelo Corolário 3.5.28, existe uma única extensão de $\mathcal{O}'$ a L. Assim, por transitividade, existe uma única extensão de $\mathcal{O}$ a L.

(1) $\Rightarrow$ (2): Seja $\widetilde{\mathcal{O}}$ a única extensão de $\mathcal{O}$ ao fecho algébrico $\widetilde{K}$ de K. Sejam $\widetilde{\mathcal{M}}$ o ideal maximal, $\overline{\widetilde{K}}$ o corpo de resíduos e

$$\widetilde{v} : \widetilde{K} \to \widetilde{\Gamma} \cup \{\infty\}$$

a valorização que correspondem a $\widetilde{\mathcal{O}}$.

Inicialmente observamos que para todo K-automorfismo σ de $\widetilde{K}$ temos que $\sigma(\widetilde{\mathcal{O}})$ é também anel de valorização de K, e portanto, como $\widetilde{\mathcal{O}}$ é o único anel de valorização de $\widetilde{K}$ estendendo $\mathcal{O}$,

$$\sigma(\widetilde{\mathcal{O}}) = \widetilde{\mathcal{O}} \quad \text{e} \quad \sigma(\widetilde{\mathcal{M}}) = \widetilde{\mathcal{M}}.$$

Pela Proposição 3.5.33(1) vale $\widetilde{v} \circ \sigma = \widetilde{v}$ para todo $K-$automorfismo σ de $\widetilde{K}$.

Em $\widetilde{K}[X]$ o polinômio f, que por hipótese é irredutível em $\mathcal{O}[X]$, se fatora completamente. Podemos então escrever f da forma

$$f(X) = \prod_{j=1}^{n} (bX - x_j), \tag{39}$$

onde $b, x_1, ..., x_n \in \widetilde{K}$, com b uma raíz $n-$ésima do coeficiente líder de f que vamos denotar por a; a qual existe por ser $\widetilde{K}$ algebricamente fechado. Além disso, note que $n \geq 1$ pois por hipótese $\overline{f} \notin \overline{K}$. Por este motivo

temos também que f é primitivo.

Como por hipótese $f \in \mathcal{O}[X]$, temos $b \in \widetilde{\mathcal{O}}$ e

$$(-1)^n x_1 ... x_n = f(0) \in \mathcal{O}. \tag{40}$$

As raízes $x_1/b, ..., x_n/b$ de f em $\widetilde{K}$ são todas $K-$conjugadas (pois pelo Lema de Gauss (Lema 3.6.2) f é também irredutível em $K[X]$), ou seja, para $1 \leq i, j \leq n$, sempre existe um $K-$automorfismo σ tal que

$$\sigma(x_i/b) = x_j/b. \tag{41}$$

Daí:

- Se algum x_i é nulo, todos os outros também o são, de modo que neste caso $f(X) = b^n X^n = aX^n \in \mathcal{O}[X]$, e da irredutibilidade de f em $\mathcal{O}[X]$ segue ainda que $n = 1$. Assim,

$$f = aX,$$

e basta então tomar $g = f$.

- Se nenhum x_i é nulo, então de $\widetilde{v} \circ \sigma = \widetilde{v}$ obtemos, para quaisquer i, j e σ satisfazendo (41),

$$\widetilde{v}(x_i/b) = (\widetilde{v} \circ \sigma)(x_i/b) = \widetilde{v}(x_j/b),$$

ou seja, existe $\gamma \in \widetilde{\Gamma}$ tal que $\widetilde{v}(x_j/b) = \gamma$ para todo $j \in \{1, ..., n\}$. Ou ainda, pondo $\delta = \gamma + \widetilde{v}(b)$ temos

$$\widetilde{v}(x_j) = \delta$$

para todo $j \in \{1, ..., n\}$. Por (40) temos $\delta \geq 0$. Segue daí que

$$\text{ou} \quad x_1, ..., x_n \in \widetilde{\mathcal{M}} \quad \text{ou} \quad x_1, ..., x_n \in \widetilde{\mathcal{O}} \backslash \widetilde{\mathcal{M}}.$$

No primeiro caso, de (39) obtemos

$$\overline{f} = (\overline{b}X)^n = \overline{b}^n X^n = \overline{a}X^n,$$

e o resultado está provado escolhendo $g(X) = X$.

No segundo caso, $\overline{x_j} \neq \overline{0}$, para todo j, e então

$$\overline{f} = \prod_{j=1}^{n} (\overline{b}X - \overline{x_j}). \tag{42}$$

Como por hipótese $\overline{f} \notin \overline{K}$, temos $\overline{b} \neq \overline{0}$.

Assim, se $\overline{f}$ não é irredutível em $\overline{K}[X]$, então $n > 1$ e podemos escrever

$$\overline{f} = \overline{g}.\overline{h}$$

para certos polinômios relativamente primos $\overline{g}$ e $\overline{h}$ com $g, h \in \mathcal{O}[X]$. Note que $\overline{x_j/b}$ são todas as raízes de $\overline{f}$ em $\widetilde{\overline{K}}$. Consideramos $\overline{x_i/b}$ uma raíz de $\overline{g}$ e $x_j \neq x_i$ tal que $\overline{x_j/b}$ é uma raíz de $\overline{h}$. Então $g(x_i/b) \in \widetilde{\mathcal{M}}$ e $h(x_j/b) \in \widetilde{\mathcal{M}}$. Tomamos $\sigma \in Gal(\widetilde{K}|K)$ tal que $\sigma(x_i/b) = x_j/b$, cuja existência é garantida por (41). Então

$$g(x_j/b) = g(\sigma(x_i/b)) = \sigma(g(x_i/b)) \in \sigma(\widetilde{\mathcal{M}}) = \widetilde{\mathcal{M}}.$$

Logo $\overline{g}$ tem também $\overline{x_j/b}$ como raiz, uma contradição com a suposição de que $\overline{h}$ e $\overline{g}$ são relativamente primos. Assim, concluímos que $\overline{f} = \overline{g}^{\,s}$, com $\overline{g}$ irredutível.

(2) $\Rightarrow$ (3): Inicialmente observamos que se $\overline{f} = \overline{g}.\overline{h}$ com $\overline{g}, \overline{h}$ relativamente primos em $\overline{K}[X]$ então f não é um polinômio constante nem um elemento de $\mathcal{M}[X]$. Em particular, f é primitivo. Assim, pelo Lema 3.6.2(4), f admite uma fatoração em irredutíveis de $\mathcal{O}[X]$, digamos,

$$f = g_1 ... g_m \quad \text{com} \quad g_1, ..., g_m \in \mathcal{O}[X],$$

irredutíveis e mais até, primitivos, pois f é primitivo.

Assim, em $\overline{K}[X]$, temos $\overline{f} = \overline{g_1} ... \overline{g_m}$. Aplicando a hipótese a cada $\overline{g_i}$, obtemos que, para todo $i \in \{1, ..., m\}$, ou $\overline{g_i} \in \overline{K}$, ou existem $a_i \in \mathcal{O}$ e $f_i \in \mathcal{O}[X]$ com $\overline{a_i} \neq \overline{0}$ e $\overline{f_i}$ irredutível em $\overline{K}[X]$ e $\overline{g_i} = \overline{a_i}\ \overline{f_i}^{\,t_i}$ para algum $t_i \geq 1$. Claramente podemos supor que os coeficientes de f_i que

pertencem a $\mathcal{M}$ são todos nulos, e assim, reenumerando convenientemente os polinômios $g_1, ..., g_m$, podemos supor que

$$\overline{g}.\overline{h} = \overline{f} = \overline{g_1}...\overline{g_m} = \overline{c} \prod_{i=1}^{l} \overline{f_i}^{t_i},$$

onde $\overline{g_i} = \overline{a_i}\ \overline{f_i}^{\ t_i}$ para $i \in \{1, ..., l\}$ e $\overline{g_j} = \overline{c_j} \in \overline{K}$ para $j \in \{l+1, ..., m\}$, e daí

$$\overline{c} = \prod_{i=1}^{l} \overline{a_i} \ . \prod_{j=l+1}^{m} \overline{g_j}$$

Como $\overline{g}$ e $\overline{h}$ são relativamente primos e $\overline{K}[X]$ é domínio de fatoração única, temos

$$\overline{a} \prod_{i=1}^{k} \overline{f_i}^{t_i} = \overline{g} \ , \ \overline{b} \prod_{i=k+1}^{l} \overline{f_i}^{t_i} = \overline{h} \ , \text{ com } \overline{a}.\overline{b} = \overline{c}$$

Definimos então

$$g_1 = a \prod_{i=1}^{k} f_i^{t_i} \quad \text{e} \quad h_1 = b \prod_{i=k+1}^{l} f_i^{t_i}.$$

Claramente g_1 e h_1 satisfazem os requisitos, inclusive a igualdade dos graus.

(3) $\Rightarrow$ (4): Sejam $g(X) = X - a$ e $\overline{h} \in \overline{K}[X]$, tais que $\overline{f} = \overline{g}.\overline{h}$. Como $\overline{f}\,'(\overline{a}) \neq 0$, $\overline{g}$ e $\overline{h}$ são relativamente primos. Por hipótese existem $g_1, h_1 \in \mathcal{O}[X]$ com

$$f = g_1.h_1 \ , \ \overline{g_1} = \overline{g} = X - \overline{a} \quad \text{e} \quad \deg(g_1) = 1 = \deg(\overline{g}).$$

Assim

$$g_1 = e(X - b)$$

com $\overline{e} = \overline{1}$ e $\overline{e.b} = \overline{a}$. Mas então $f(b) = 0$ e $\overline{b} = \overline{a}$ com $b \in \mathcal{O}$.

(4) $\Rightarrow$ (5) : Temos que

$$f(a-X) = f(a) - f'(a)X + X^2 g(X),$$

para algum $g \in \mathcal{O}[X]$. Fazemos agora uma mudança de variáveis definida por $X = f'(a)Y$ e, como $v(f'(a)) = \infty$ não pode ocorrer, podemos reescrever a igualdade acima da seguinte forma:

$$\frac{f(a-f'(a)Y)}{f'(a)^2} = \frac{f(a)}{f'(a)^2} - Y + Y^2 g(f'(a)Y). \tag{43}$$

Definimos

$$h(Y) = g(f'(a)Y) \quad \text{e} \quad f_1(Y) = \frac{f(a)}{(f'(a))^2} - Y + Y^2 h(Y),$$

obtendo

$$\frac{f(a-f'(a)Y)}{f'(a)^2} = f_1(Y) = \frac{f(a)}{f'(a)^2} - Y + Y^2 h(Y). \tag{44}$$

Como $f'(a) \in \mathcal{O}$ e $g \in \mathcal{O}[X]$, temos $h(Y) \in \mathcal{O}[Y]$; ainda, como $v(f(a)) > v(f'(a)^2)$ temos também $f_1(Y) \in \mathcal{O}[Y]$. Em $\overline{K}[Y]$ obtemos

$$\overline{f_1} = Y(Y\overline{h}(Y) - \overline{1})$$

que tem $\overline{0}$ como raiz simples. Portanto, da hipótese concluímos que f_1 tem uma raiz $b \in \mathcal{M}$. Então, fazendo $Y = b$ na equação (44), concluímos que f tem $\alpha = a - f'(a)b \in \mathcal{O}$ para raiz. Como $b \in \mathcal{M}$, vale também que $v(\alpha - a) > v(f'(a))$.

(5) $\Rightarrow$ (6) : Denotando por f o polinômio $f = X^n + a_{n-1}X^{n-1} + ... + a_0$, obtemos

$$\overline{f} = X^n + \overline{a_{n-1}}X^{n-1} = X^{n-1}(X + \overline{a_{n-1}}).$$

Portanto $-\overline{a_{n-1}}$ ($\neq \overline{0}$ por hipótese) é um zero simples de $\overline{f}$. Em particular,

$$v(f(-a_{n-1})) > 0 = v(f'(-a_{n-1})) = 2v(f'(-a_{n-1})).$$

Então da hipótese concluímos que f tem um zero em $\mathcal{O}$.

(6) $\Rightarrow$ (7) : É claro.

(7) $\Rightarrow$ (6) : Denotemos por f o polinômio $X^n + a_{n-1}X^{n-1} + ... + a_0$. Substituindo X por $a_{n-1}Y$ e dividindo por a_{n-1}^n obtemos

$$\frac{f(a_{n-1})}{a_{n-1}^n} = Y^n + Y^{n-1} + \frac{a_{n-2}}{a_{n-1}^2}Y^{n-2} + ... + \frac{a_0}{a_{n-1}^n} =: g(Y).$$

Note que os coeficientes de $g(Y)$ diferentes de 1 ainda são elementos de $\mathcal{M}$.

Então a hipótese nos garante que $g(Y)$ tem uma raiz $b \in \mathcal{O}$. Daí $a = a_{n-1}b \in \mathcal{O}$ é uma raiz de f.

(6) $\Rightarrow$ (1) : Suponha que existe uma extensão algébrica de K que admite mais de um prolongamento de $\mathcal{O}$ a cla. Então existe uma extensão de Galois finita $N|K$ com grupo de Galois $G(N|K)$, na qual $\mathcal{O}$ tem mais do que uma extensão.

De fato, se $\mathcal{O}$ possui mais de um prolongamente então possui mais de um prolongamento ao fecho algébrico de K e portanto ao seu fecho separável K^s. Logo, existem $y \in K^s$ e v_1', v_2' valorizações de K^s tais que $v_1'(y) \neq v_2'(y)$. Assim (tomando o fecho normal de $K(y)$, por exemplo), existe uma extensão Galoisiana finita $N|K$ na qual $\mathcal{O}$ admite mais de um prolongamento.

Seja $\mathcal{O}^*$ um prolongamento de $\mathcal{O}$ a N. Definimos

$$H = \{\sigma \in G(N|K) \mid \sigma(\mathcal{O}^*) = \mathcal{O}^*\}.$$

Já que $\mathcal{O}^*$ não é o único prolongamento de $\mathcal{O}$ a N, o grupo H é um subgrupo próprio de $G(N|K)$, e logo o corpo L fixado por H é uma extensão própria de K. Tomamos agora o conjunto $\{\mathcal{O}^* = \mathcal{O}_1, ..., \mathcal{O}_m\}$ de todos os conjugados distintos de $\mathcal{O}^*$ em N. Definimos $\mathcal{O}_i' = \mathcal{O}_i \cap L$ para $1 \leq i \leq m$ e consideramos o seguinte subanel de L,

$$R = \mathcal{O}_1' \cap ... \cap \mathcal{O}_m'.$$

Pelo Teorema 3.4.14 e pelo Lema 3.5.22, os ideais maximais de R são todos da forma $\mathfrak{p}_i = R \cap \mathcal{M}_i = R \cap \mathcal{M}_i$. Note porém que no nosso caso podemos ter $\mathfrak{p}_i = \mathfrak{p}_j$ para $i \neq j$, já que não temos garantias de que $\mathcal{O}_i' \not\subseteq \mathcal{O}_j'$ para todo $i \neq j$, porém este não é o caso se $i = 1$. De fato, se $\mathfrak{p}_1 = \mathfrak{p}_j$ então

$$\mathcal{O}^* \cap L = \mathcal{O}_1' \overset{\text{Lema 3.4.13}}{=} R_{\mathfrak{p}_1} = R_{\mathfrak{p}_j} \overset{\text{Lema 3.4.13}}{=} \mathcal{O}_j' = \mathcal{O}_j \cap L.$$

E pelo Teorema da Conjugação 3.5.32 temos $\mathcal{O}_j = \sigma(\mathcal{O}^*)$ para algum $\sigma \in G(N/L) = H$. Assim $\mathcal{O}_j = \mathcal{O}^*$ pela definição de H.

Assim, usando o Teorema 3.4.14 encontramos $\beta \in R$ com $\beta - 1 \in \mathcal{M}_1' \subset \mathcal{M}_1$ e $\beta \in \mathcal{M}_i' \subset \mathcal{M}_i$ para todo $i \in \{2, ..., m\}$. Observamos que no caso de $\mathcal{O}_i' = \mathcal{O}_j'$, para certos $i \neq j$, temos $\mathcal{M}_i = \mathcal{M}_j$, o que não influencia nas condições exigidas acima.

Seja $\{\beta = \beta_1, ..., \beta_n\}$ o conjunto de todos os elementos K-conjugados a β em N (que são dois a dois distintos pois a extensão $N|K$ é separável) e seja

$$Irr(\beta, K) = X^n + a_{n-1}X^{n-1} + ... + a_0 \in K[X].$$

o seu polinômio minimal.

- *Afirmação 1*: $\beta_j \neq \beta_1 \Rightarrow \beta_j = \tau(\beta)$ para algum $\tau \in G(N|K) \backslash H$.

De fato, como $\beta \in R \subset L$ e L é o corpo fixo por H, se existisse $\tau \in H$ com

$$\beta_j = \tau(\beta) \in \mathcal{O}^* = \mathcal{O}_1,$$

então $\beta = \beta_j$, o que contradiz a escolha de β_j.

- *Afirmação 2*: $\beta_j \in \mathcal{M}_1$ para todo $j \geq 2$.

De fato, pela *Afirmação 1*, $\beta_j = \tau(\beta)$, $\tau \notin H$. Portanto $\tau^{-1}(\mathcal{O}_1) = \mathcal{O}_i$ para algum $1 \leq i \leq m$. Como pela condição de aproximação $\beta \in \mathcal{M}_i = \tau^{-1}(\mathcal{M}_1)$, temos $\beta_j = \tau(\beta) \in \tau(\tau^{-1}(\mathcal{M}_1)) = \mathcal{M}_1$.

- *Afirmação 3*: $1 + a_{n-1} \in \mathcal{M}_1$ (e portanto $a_{n-1} \notin \mathcal{M}$) e $a_{n-2}, ..., a_0 \in \mathcal{M}_1$.

De fato, como $a_{n-1} = -(\beta_1 + ... + \beta_n)$, e $1 - \beta_1 \in \mathcal{M}_1$, pelas *Afirmações 1 e 2* temos

$$1 + a_{n-1} = \underbrace{(1 - \beta_1)}_{\in \mathcal{M}_1} - \underbrace{\beta_2 - ... - \beta_n}_{\in \mathcal{M}_1} \in \mathcal{M}_1,$$

Claramente, de $\beta_j \in \mathcal{M}_1$ para todo $j \geq 2$ (*Afirmação 2*) e de $\beta_1 \in \mathcal{O}_1$, obtemos que $a_{n-2}, ..., a_0 \in \mathcal{M}_1$.

Portanto

$$f = Irr(\beta, K) = X^n + a_{n-1}X^{n-1} + ... + a_0,$$

pela condição (6), deve ter uma raiz em K.

Por outro lado, como $m > 1$, as raízes de f não podem estar em K. Esta contradição prova a implicação.

■

Definição 3.6.5 *Um corpo valorizado $(K, \mathcal{O})$ é dito Henseliano se satisfaz alguma (e portanto todas) condição do Teorema 3.6.4.*

Também nos referimos ao respectivo anel $\mathcal{O}$ de um corpo valorizado henseliano $(K, \mathcal{O})$ como anel henseliano (de K).

Na definição acima, levando em conta a condição (1) do teorema, é claro que basta requerer a unicidade da extensão apenas para as extensões finitas.

Segue da definição que a propriedade de ser henseliano é *hereditária*, ou seja, para qualquer extensão algébrica de corpos valorizados $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$, se $(K_1, \mathcal{O}_1)$ é henseliano, então também o é $(K_2, \mathcal{O}_2)$.

O objetivo a partir de agora é provar que todo corpo valorizado possui uma extensão algébrica que seja henseliana.

Definição 3.6.6 *Sejam $L|K$ uma extensão Galoisiana de corpos com $G := Gal(L|K)$ e $\mathcal{O}$ um anel de valorização em K e $\mathcal{O}'$ uma extensão de $\mathcal{O}$ a*

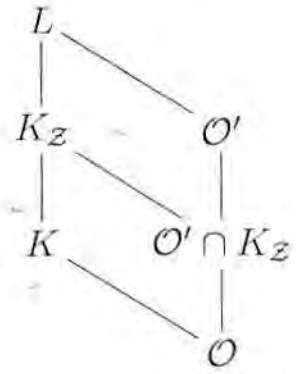
L. O subgrupo

$$\mathcal{Z}(\mathcal{O}') := \{\tau \in G \mid \tau(\mathcal{O}') = \mathcal{O}'\} \subseteq Gal(L|K)$$

é chamado o grupo de decomposição de $\mathcal{O}'|\mathcal{O}$. *O corpo*

$$K_{\mathcal{Z}} := \{z \in L \mid \sigma(z) = z, \text{ para todo } \sigma \in \mathcal{Z}(\mathcal{O}')\}$$

fixado por $\mathcal{Z}(\mathcal{O}')$ *é chamado o corpo de decomposição de* $\mathcal{O}'|\mathcal{O}$.



Se L é o fecho separável de K, isto é $L = K^s$, *então* $(K_{\mathcal{Z}}, \mathcal{O}' \cap K_{\mathcal{Z}})$ *é chamado o fecho henseliano ou henselização de* $(K, \mathcal{O})$ *(em* $(L, \mathcal{O}')$*).*

Queremos mostrar que a henselização de $(K, \mathcal{O})$ é a extensão algébrica que buscamos:

Teorema 3.6.7

(*i*) *A Henselização* $(K_{\mathcal{Z}}, \mathcal{O}_{\mathcal{Z}})$ *de* $(K, \mathcal{O})$ *é um corpo henseliano. Em particular, todo corpo valorizado admite uma extensão algébrica que é henseliana.*

(*ii*) $(K_{\mathcal{Z}}, \mathcal{O}_{\mathcal{Z}})$ *é uma extensão imediata de* $(K, \mathcal{O})$.

Prova. Dividimos em dois casos:

1°caso: $K^s|K$ é finita.

Neste caso, $G = Gal(K^s|K)$ é finito. Sejam $H = \mathcal{Z}(\mathcal{O}')$ e $m = [G : H]$. Escrevemos G então como união disjunta de classes laterais determinadas

por H na forma

$$G = \sigma_1^{-1}H \cup ... \cup \sigma_m^{-1}H, \tag{45}$$

para convenientes $\sigma_i \in G$ e, sem perda de generalidade tomamos $\sigma_1 = id$.

Assim, temos que

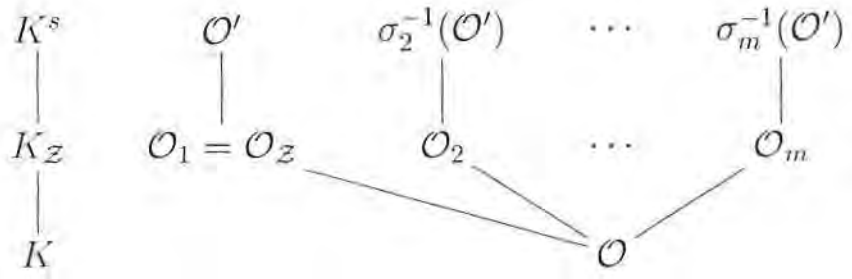
$$\mathcal{O}', \sigma_2^{-1}\mathcal{O}', ..., \sigma_m^{-1}\mathcal{O}'$$

são extensões de $\mathcal{O}$ a K^s. Novamente, pelo Teorema da Conjugação 3.5.32, não existem outras além destas. E não existem repetições na lista, pela maneira que escolhemos $\sigma_1, ..., \sigma_m$.

Escrevemos agora $K_Z^i = \sigma_i(K_Z)$ para $i \in \{1, ..., n\}$. Assim

$$K_Z^1 = \sigma_1(K_Z) = K_Z \quad \text{e} \quad \mathcal{O}_i := \sigma_i^{-1}(\mathcal{O}') \cap K_Z$$

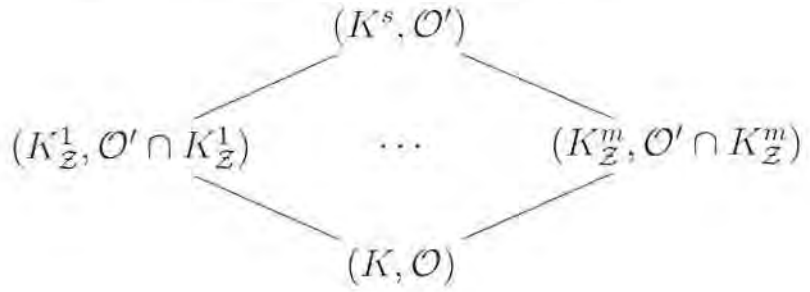
é um anel de valorização de K_Z.



Observamos também que, por outro lado,

$$\sigma_i(\mathcal{O}_i) = K_Z^i \cap \mathcal{O}', \tag{46}$$

o que nos permite construir o seguinte diagrama



Afirmação 1 : $\mathcal{O}'$ é a única extensão de $\mathcal{O}_1 = \mathcal{O}' \cap K_Z = \mathcal{O}_Z$ a K^s, e portanto $(K_Z, \mathcal{O}_1)$ é henseliano.

De fato, se

$$\mathcal{O}_i = \sigma_i^{-1}(\mathcal{O}') \cap K_{\mathcal{Z}}$$

fosse igual a

$$\mathcal{O}_1 = \mathcal{O}' \cap K_{\mathcal{Z}},$$

então, pelo Teorema 3.5.31, deveria existir $\tau \in Aut(K^s|K_{\mathcal{Z}}) = H$ com

$$\tau\sigma_i^{-1}(\mathcal{O}') = \mathcal{O}'$$

Mas então $\tau\sigma_i^{-1} \in \mathcal{Z}(\mathcal{O}') = H$, ou seja,

$$\tau \in H \text{ e } \tau\sigma_i \in H \Rightarrow \sigma_i^{-1} \in H.$$

Portanto , pela escolha dos σ_i, concluímos que $\sigma_i = id$.

Para as próximas afirmações relativas a este caso consideramos

$$R = \bigcap_{i=1}^{m} \mathcal{O}_i \overset{(46)}{=} \bigcap_{i=1}^{m} \sigma_i^{-1}(\mathcal{O}' \cap K_{\mathcal{Z}}^i) \subseteq K_{\mathcal{Z}}.$$

Afirmação 2: O grau residual $f(\mathcal{O}_1|\mathcal{O}) = 1$.

De fato, dado $\alpha \in \mathcal{O}_1$, queremos mostrar que existe um $a \in \mathcal{O}$ com $\alpha - a \in \mathcal{M}_1$, onde $\mathcal{M}_1$ é o ideal maximal de $\mathcal{O}_1$; para isto, escolhemos $\beta \in R$ tal que

$$\beta - \alpha \in \mathcal{M}_1 \tag{47}$$

e

$$\beta \in \mathcal{M}_i = \sigma_i^{-1}(\mathcal{M}') \cap K_{\mathcal{Z}} \tag{48}$$

para $i \in \{2, ..., m\}$. Tal β existe pelo Teorema 3.4.14(3). Definimos

$$a = \sum_{i=1}^{m} \sigma_i(\beta). \tag{49}$$

Então $a \in K$, pois afirmamos que a é invariante por todos os elementos de G. De fato, para qualquer $\sigma \in G$, os elementos $\sigma\sigma_1, ..., \sigma\sigma_m$ formam um outro sistema de representantes das classes laterais de G/H, os quais, após

eventual reordenação, aplicam β nas mesmas imagens de β mapeadas por $\sigma_1, ..., \sigma_m$. Usamos aí também o fato que $\beta \in R \subseteq K_{\mathcal{Z}}$. Portanto, visto que $a, \beta \in K_{\mathcal{Z}}$, por escolha, e $\sum_{i=2}^{m} \sigma_i(\beta) \in \mathcal{M}'$ por (49) e (48), temos

$$a - \beta = \sum_{i=2}^{m} \sigma_i(\beta) \in \mathcal{M}' \cap K_{\mathcal{Z}} = \mathcal{M}_1,$$

o que implica

$$a - \alpha = (a - \beta) + (\beta - a) \in \mathcal{M}_1,$$

usando (47).

Afirmação 3 : O índice de ramificação $e(\mathcal{O}_1|\mathcal{O}) = 1$.

De fato, para cada $\alpha \in K_{\mathcal{Z}}^{\times}$ afirmamos que existe um $a \in K^{\times}$ com $v_1(\alpha) = v_1(a) = v(a)$. Para isto, escolhemos $\beta \in R$ com

$$1 - \beta \in \mathcal{M}_1 \quad \text{e} \quad \beta \in \mathcal{M}_i$$

para $i \in \{2, ..., m\}$, o que é possível pelo Teorema 3.4.14. Portanto

$$v_1(\beta) = 0 \quad \text{e} \quad v_i(\beta) > 0$$

para $i \in \{2, ..., m\}$, ou seja,

$$v'(\beta) = 0 \quad \text{e} \quad v'(\sigma_i(\beta)) > 0 \tag{50}$$

para $i \in \{2, ..., m\}$, onde v' é a valorização de K^s associada a $\mathcal{O}'$.

Portanto, por (50), existem números $n \in \mathbb{Z}$ tais que

$$v'(\beta^n \alpha) = v'(\alpha) \neq n.v'(\sigma_i(\beta)) + v'(\sigma_i(\alpha)) = v'(\sigma_i(\beta^n \alpha)) \tag{51}$$

para todo $i = 2, ..., m$.

Tomando $\alpha_n := \beta^n \alpha$, com $n \in \mathbb{Z}$ escolhido satisfazendo (51), obtemos que $v'(\alpha_n) \neq v'(\sigma_i(\alpha_n))$ para $i \in \{2, ..., m\}$. Fixamos para tal n o conjunto

$$W_n = \{i \mid i \in \{2, ..., m\} \text{ e } v'(\sigma_i(\alpha_n)) < v'(\alpha_n)\} \subseteq \{2, ..., m\},$$

e fixamos $w_n = \mathsf{card}(W_n)$.

Definimos agora para cada $w \in \{1, ..., m\}$ e $\gamma \in K^s$:

$$r_w := \sum_{\substack{I \subseteq \{1,...,m\} \\ \mathrm{card}(I)=w}} \prod_{i \in I} \sigma_i(\gamma). \tag{52}$$

Assim

$$v'(r_{w_n}) = v'\left(\prod_{i \in W_n} \sigma_i(\alpha_n)\right),$$

pois as outras parcelas em r_{w_n} tem valor maior do que $v'\left(\prod_{i \in W_n} \sigma_i(\alpha_n)\right)$. Também temos

$$v'(r_{w_n+1}) = v'\left(\alpha_n \prod_{i \in W_n} \sigma_i(\alpha_n)\right).$$

Portanto

$$a := \frac{r_{w_n+1}}{r_{w_n}} \in K,$$

pois por (52) temos $r_{w_n}, r_{w_n+1} \in K$. Com isto vale

$$v(a) = v'(a) = v'(\alpha_n) \overset{(51)}{=} v'(\alpha) = v_1(\alpha)$$

como queríamos.

Passamos para o segundo caso, o mais geral.

2^ocaso: $K^s|K$ é arbitrária.

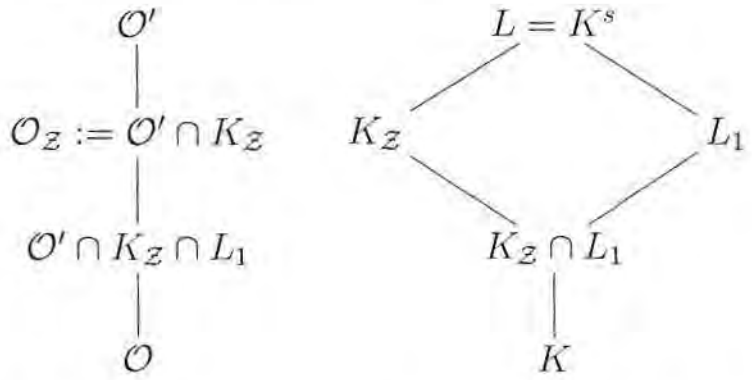
Escolhemos $L_1|K$ uma extensão Galoisiana finita com $L_1 \subset L$. Tomamos $G_1 = Gal(L_1|K)$ e

$$\mathcal{Z}_1(\mathcal{O}') = \{\sigma \in G_1 \mid \sigma(\mathcal{O}' \cap L_1) = \mathcal{O}' \cap L_1\}.$$

Denotando por $\mathfrak{F}(H)$ o subcorpo de K^s fixado por H, para todo subgrupo $H \subset G$, temos, pelo Teorema da Conjugação 3.5.32, que

$$\mathfrak{F}(\mathcal{Z}_1(\mathcal{O}')) = L_1 \cap \mathfrak{F}(\mathcal{Z}(\mathcal{O}')) = L_1 \cap K_{\mathcal{Z}},$$

Assim temos os seguintes diagramas:



Afirmação $1'$: $\mathcal{O}'$ é a única extensão de $\mathcal{O}_Z = \mathcal{O}' \cap K_Z$ a K^s, e portanto $(K_Z, \mathcal{O}_Z)$ é henseliano.

De fato, supomos que $\mathcal{O}''$ é uma outra extensão de $\mathcal{O}_Z$ a K^s e que podemos encontrar um $\alpha \in \mathcal{O}' \backslash \mathcal{O}''$. Se $L_1|K$ é uma extensão Galois com $\alpha \in L_1 \subseteq L$ então

$$\mathcal{O}' \cap K_Z \cap L_1 = \mathcal{O}'' \cap K_Z \cap L_1 \quad \text{e} \quad \alpha \in (\mathcal{O}' \cap L_1) \backslash (\mathcal{O}'' \cap L_1),$$

o que contradiz a *Afirmação 1.*

Afirmação $2'$: O grau residual é $f(\mathcal{O}_Z|\mathcal{O}) = 1$.

De fato, seja $\alpha \in \mathcal{O}_Z$ com $\alpha + \mathcal{M}_Z \notin \mathcal{O}/\mathcal{M}$. Escolha uma extensão Galois finita $L_1|K$ com $\alpha \in L_1 \subseteq L$ e então conseguimos contradizer a *Afirmação 2.*

Afirmação $3'$: O índice de ramificação é $e(\mathcal{O}_Z|\mathcal{O}) = 1$.

De fato, seja $\alpha \in K_Z^\times$ com $v_Z(\alpha) \notin v(K)$. Escolha uma extensão Galois finita $L_1|K$ com $\alpha \in L_1 \subseteq L$ e então conseguimos contradizer a *Afirmação 3* .

Com todas as afirmações acima temos provado o teorema.

■

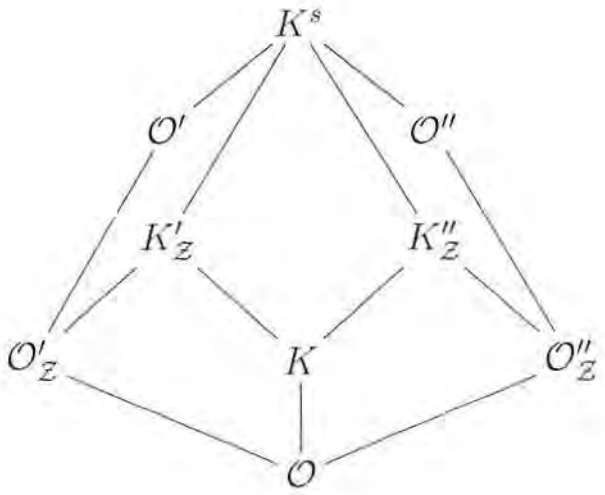
Observação 3.6.8 *A Henselização $(K_Z, \mathcal{O}_Z)$ de $(K, \mathcal{O})$ é determinada pelas extensões $\mathcal{O}'$ de $\mathcal{O}$ em K^s.*

De fato, pelo Teorema da Conjugação (Teorema 3.5.32), se $\mathcal{O}$ e $\mathcal{O}'$ são duas extensões então existe um K-automorfismo λ de K^s tal que $\lambda(\mathcal{O}') = \mathcal{O}''$. Denotando por $K'_{\mathcal{Z}}$ e $K''_{\mathcal{Z}}$ os corpos fixos por $\mathcal{Z}(\mathcal{O}')$ e $\mathcal{Z}(\mathcal{O}'')$, respectivamente.

Afirmamos que

$$\lambda(K'_{\mathcal{Z}}) = K''_{\mathcal{Z}}, \tag{53}$$

de modo que $(K_{\mathcal{Z}}, \mathcal{O}_{\mathcal{Z}})$ fica bem determinado a menos de K-isomorfismos, ou seja, a henselização é única a menos de K-isomorfismos.



De fato,

$$\mathcal{Z}(\mathcal{O}'') = \lambda \mathcal{Z}(\mathcal{O}')\lambda^{-1}, \tag{54}$$

pois

$$\tau \in \mathcal{Z}(\mathcal{O}') \;\Rightarrow\; \lambda\tau\lambda^{-1}(\mathcal{O}'') = \mathcal{O}'' \;\Rightarrow\; \lambda\tau\lambda^{-1} \in \mathcal{Z}(\mathcal{O}'')$$

e

$$\sigma \in \mathcal{Z}(\mathcal{O}'') \;\Rightarrow\; \lambda^{-1}\sigma\lambda \in \mathcal{Z}(\mathcal{O}'),$$

digamos, $\lambda^{-1}\sigma\lambda = \tau$, e então $\sigma = \lambda\tau\lambda^{-1} \in \lambda\mathcal{Z}(\mathcal{O}')\lambda^{-1}$.

Agora, de (54) obtemos (53). Para tal, observe que para todo $\tau \in \mathcal{Z}(\mathcal{O}'')$ e todo $x \in K'_{\mathcal{Z}}$ temos que $\lambda^{-1}\tau\lambda(x) = x$ por (54), ou seja,

$$\tau(\lambda(x)) = \lambda(x) \;\; \textit{para todo} \;\; \tau \in \mathcal{Z}(\mathcal{O}''),$$

o que implica que $\lambda(x) \in K''_{\mathcal{Z}}$ (o corpo fixo por $\mathcal{Z}(\mathcal{O}'')$). A outra inclusão

é análoga.

Relembrando a Definição 3.6.5 de corpo henseliano, vemos que se K tem $\mathcal{O}$ como anel de valorização trivial então $\mathcal{O} = K$ e $(K, \mathcal{O})$ é henseliano, já que pelo Lema 3.5.20, a valorização trivial estende-se apenas para triviais para uma extensão algébrica.

Passamos agora à caracterização da henselização.

Teorema 3.6.9 *A Henselização $(K_{\mathcal{Z}}, \mathcal{O}_{\mathcal{Z}})$ de um corpo valorizado $(K, \mathcal{O})$ tem a seguinte caracterização:*

(1) *$(K_{\mathcal{Z}}, \mathcal{O}_{\mathcal{Z}})$ é Henseliano,*

(2) *Se $(K, \mathcal{O}) \subseteq (K_1, \mathcal{O}_1)$ e $(K_1, \mathcal{O}_1)$ é Henseliano, então existe uma imersão univocamente determinada*

$$\lambda : (K_{\mathcal{Z}}, \mathcal{O}_{\mathcal{Z}}) \to (K_1, \mathcal{O}_1) \quad com \quad \lambda|_K = id.$$

Prova. O Teorema 3.6.7 nos garante (1). Para mostrar (2) observamos que, uma vez que, pelo Corolário 3.5.28, todo subcorpo relativamente separavelmente fechado de $(K_1, \mathcal{O}_1)$ é também Henseliano com respeito à valorização induzida de K_1, é suficiente considerar o caso em que $K_1|K$ é separável.

Seja $\mathcal{O}^s$ a extensão unicamente determinada de $\mathcal{O}_1$ em K^s. Então

$$K_0 := \mathfrak{F}(\mathcal{Z}(\mathcal{O}^s)) \subseteq K_1.$$

pois se $\sigma \in Gal(K^s|K_1)$ temos $\sigma(\mathcal{O}^s) = \mathcal{O}^s$, pois K_1 é henseliano e então $\sigma \in \mathcal{Z}(\mathcal{O}^s)$. Portanto $Gal(K^s|K_1) \subset \mathcal{Z}(\mathcal{O}^s)$, donde

$$\mathfrak{F}(\mathcal{Z}(\mathcal{O}^s)) \subseteq \mathfrak{F}(Gal(K^s|K_1)) = K_1.$$

Como $\mathcal{O}'$ e $\mathcal{O}^s$ são ambos extensões de $\mathcal{O}$ a K^s, então existe um $\lambda \in Gal(K^s|K)$ com $\lambda(\mathcal{O}') = \mathcal{O}^s$. No entanto

$$\lambda(K_{\mathcal{Z}}) = \lambda(\mathfrak{F}(\mathcal{Z}(\mathcal{O}'))) = \mathfrak{F}(\mathcal{Z}(\mathcal{O}^s)) = K_0 \subset K_1$$

e $\mathcal{Z}(\mathcal{O}^s) = \lambda\mathcal{Z}(\mathcal{O}')\lambda^{-1}$. Também, λ é unicamente determinada, pois se fosse

$$\rho : K_{\mathcal{Z}} \to K_0,\ \rho|_K = id,\ \text{e}\ \rho(\mathcal{O}_{\mathcal{Z}}) = \mathcal{O}^s \cap K_0 =: \mathcal{O}_0.$$

Estendemos ρ para K^s, e então

$$K_{\mathcal{Z}} \cap \lambda^{-1}(\mathcal{O}^s) = \mathcal{O}_{\mathcal{Z}} = K_{\mathcal{Z}} \cap \rho^{-1}(\mathcal{O}^s),$$

portanto

$$\mathcal{O}' = \lambda^{-1}(\mathcal{O}^s) = \rho^{-1}(\mathcal{O}^s) = \rho^{-1}\lambda(\mathcal{O}').$$

Por isto $\rho^{-1}\lambda \in \mathcal{Z}(\mathcal{O}')$ e com isto $\lambda|_{K_{\mathcal{Z}}} = \rho|_{K_{\mathcal{Z}}}$.

■

Definição 3.6.10 *Um corpo valorizado $(K, \mathcal{O})$ é chamado algebricamente maximal se não admite nenhuma extensão algébrica imediata própria $(K', \mathcal{O}')$.*

Note que K com a valorização trivial é algebricamente maximal.

Um corpo valorizado henseliano nem sempre é algebricamente maximal. Estabelecemos a seguir uma condição suficiente para garantir esta propriedade.

Definição 3.6.11 *Um corpo valorizado $(K, \mathcal{O})$ é dito finitamente ramificado se*

(1) $\mathsf{car}(\overline{K}) = 0$, *ou*

(2) $\mathsf{car}(\overline{K}) = p > 0$ *e existem somente finitos valores entre* 0 *e* $v(p)$.

Observação 3.6.12 *Note que $(K, \mathcal{O})$ com $\mathcal{O} = K$ é finitamente ramificado — pois neste caso a valorização associada é identicamente nula; também se $(K, \mathcal{O})$ é finitamente ramificado e $\mathcal{O}$ é não trivial, então K é um corpo infinito e afirmamos que $\mathsf{car}(K) = 0$. De fato, se $\mathsf{car}(\overline{K}) = 0$ então é claro que $\mathsf{car}(K) = 0$; e, se $\mathsf{car}(\overline{K}) = \mathsf{car}(K) = p > 0$, então $v(p) = v(0) = \infty$ e existem infinitos valores entre* 0 *e* $v(p)$, *pois $\mathcal{O}$ é não trivial e K é infinito.*

Exemplo 3.6.13 *Se o grupo de valores associado a* $(K, \mathcal{O})$ *é isomorfo a* $\mathbb{Z}$ *e* $\mathsf{car}(K) = 0$, *então* $(K, \mathcal{O})$ *é finitamente ramificado. Basta neste caso considerar um uniformizador.*

Este é o caso do Exemplo 3.2.24 das séries formais quando consideramos K *um corpo de carcterística zero.*

Lema 3.6.14 *Se* $(K, \mathcal{O})$ *é finitamente ramificado então para todo* $n \in \mathbb{Z}\backslash\{0\}$ *existe apenas um número finito de valores entre* 0 *e* $v(n)$.

Prova. Para ver isto consideramos os dois casos $\mathsf{car}(\overline{K}) = p$ e $\mathsf{car}(\overline{K}) = 0$.

Se $\mathsf{car}(\overline{K}) = p$ escrevemos $n = p^{\,e}s$ com $p \nmid s$. Note que, como $p \nmid s$, podemos escrever

$$s = q.p + r \quad , \quad 0 < r < p,$$

com isto, tomado "barras" e lembrando que $\mathsf{car}(\overline{K}) = p$, obtemos

$$\overline{s} = \overline{q}.\overline{p} + \overline{r} = \overline{r} \neq \overline{0},$$

e portanto $v(s) = 0$.

Então

$$v(n) = e.v(p).$$

Assim, entre 0 e $v(n)$ existem no máximo "e" vezes o número de valores entre 0 e $v(p)$.

Agora suponha $\mathsf{car}(\overline{K}) = 0$. Neste caso $\mathsf{car}(K) = 0$, e portanto

$$\mathbb{Q} \subseteq K \quad \text{e} \quad \mathcal{M}_{\mathcal{O}} \cap \mathbb{Q} = (0) \subseteq \mathcal{O},$$

e assim $\overline{r} = r$ para todo $r \in \mathbb{Q}$. Em particular temos $\overline{n} = n \neq 0$, e portanto $v(n) = 0$. Logo também neste caso, existem somente finitos valores entre 0 e $v(n)$.

■

Lema 3.6.15 *Seja* $v : K \to \Gamma \cup \{\infty\}$ *uma valorização cujo anel de valorização associado é* $\mathcal{O}$, *e seja* σ *um automorfismo de* K *que fixa* $\mathcal{O}$, *ou*

seja,

$$\sigma(\mathcal{O}) = \mathcal{O}.$$

Então:

(1) *Existe um único isomorfismo de ordem* $\rho : \Gamma \to \Gamma$ *tal que, para todo* $x \in K^*$,

$$\rho(v(x)) = v(\sigma(x)).$$

(2) *Se* σ *tem ordem finita no grupo* $Aut(K)$ *ou se existe um subcorpo* F *de* K *tal que* $\sigma|_F = id_F$ *e* $v(F) = v(K)$, *então*

$$\rho = id|_\Gamma$$

Prova. (1) Claramente $(v \circ \sigma)$ define uma valorização em K com anel de valorização $\sigma(\mathcal{O}) = \mathcal{O}$ e grupo de valores $\Gamma = K^\times/\mathcal{O}^\times$. Pela Proposição 3.3.26, existe um isomorfismo $\rho : \Gamma \to \Gamma$ que preserva a ordem e tal que $\rho(v(x)) = v(\sigma(x))$, e como a igualdade da direita depende apenas de v e σ, tal isomorfismo é único.

(2) Suponha que existe $n \in \mathbb{N}$ tal que $\sigma^n = id$ e que $\rho \neq id|_\Gamma$. Existe então $x_0 \in K$ tal que $\rho(v(x_0)) = v(\sigma(x_0)) \neq v(x_0)$, onde ρ é o isomorfismo único garantido em (1). Sem perda de generalidade supomos $\rho(v(x_0)) > v(x_0)$, pois senão basta trocar x_0 por x_0^{-1}. Assim,

$$\rho^n(v(x_0)) > ... > \rho^2(v(x)) > \rho(v(x_0)) > v(x_0). \tag{55}$$

Por outro lado, temos que para todo $x \in K$ vale

$$v(x) = v(\sigma^n(x)) = \rho(v(\sigma^{n-1}(x))) = \rho^2(v(\sigma^{n-2}(x))) = ... = \rho^n(v(x)).$$

Em particular, $v(x_0) = \rho^n(v(x_0)) \overset{(55)}{>} v(x_0)$, uma contradição. Assim concluímos que $\rho = id|_\Gamma$.

No caso de $\sigma|_F = id_F$ e $v(F) = v(K)$ com $F \subseteq K$ basta observar que, como para todo $x \in K$ existe $y \in F$ tal que $v(x) = v(y)$, podemos escrever

$$\rho(v(x)) = \rho(v(y)) \overset{(1)}{=} v(\sigma(y)) \overset{y \in F}{=} v(y) = v(x),$$

ou seja, $\rho = id|_\Gamma$.

■

Teorema 3.6.16 *Suponha $(K, \mathcal{O})$ é finitamente ramificado. Então $(K, \mathcal{O})$ é Henseliano se e somente se $(K, \mathcal{O})$ é algebricamente maximal.*

Prova. ($\Leftarrow$) Seja $(K, \mathcal{O})$ algebricamente maximal. Então, pela Definição 3.6.10, $(K, \mathcal{O})$ é Henseliano, já que a Henselização de $(K, \mathcal{O})$ é uma extensão algébrica imediata de $(K, \mathcal{O})$, pelo Teorema 3.6.7.

($\Rightarrow$) Seja $(K', \mathcal{O}') \supseteq (K, \mathcal{O})$ uma extensão algébrica imediata própria. Então $\mathcal{O} \neq K$, e portanto, pela Observação 3.6.12, $\mathsf{car}(K) = 0$ (pois caso contrário a valorização associada seria a trivial e a extensão seria imediata).

Seja $\alpha \in K' \backslash K$. Sem perda de generalidade supomos que $K'|K$ é finita. Seja L o fecho normal de $K'|K$. Então $\mathcal{O}$ estende-se unicamente para L, uma vez que K é henseliano. Em particular esta extensão também estende $\mathcal{O}' \subseteq K'$ em L. Agora, para todo $\beta \in L$ e $\sigma \in G := Gal(L|K)$,

$$v(\beta) = v(\sigma(\beta)), \tag{56}$$

por (2) do Lema 3.6.15.

Sejam $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n$ os conjugados de α. Então sabemos que para todo $b \in K$ temos

$$v(\alpha_i - b) = v(\sigma(\alpha - b)) \overset{(56)}{=} v(\alpha - b). \tag{57}$$

Definimos

$$a := \frac{1}{n}\sum_{i=1}^{n} \alpha_i \in K. \tag{58}$$

Como $\alpha \notin K$, temos

$$\alpha - a \neq 0;$$

ainda, como $(K', \mathcal{O}')$ é uma extensão imediata de $(K, \mathcal{O})$,

$$v(\alpha - a) \in v(K') = v(K),$$

ou seja, existe um $c \in K$ com $v(c) = v(\alpha - a)$, e portanto

$$v\left(\frac{\alpha - a}{c}\right) = 0.$$

Mas também $\overline{K'} = \overline{K}$, e portanto existe um $d \in K$ com

$$v\left(\frac{\alpha - a}{c} - d\right) > 0.$$

Segue então que

$$v(\alpha - \underbrace{(a + cd)}_{=:\, a_1 \in K}) > v(c) = v(\alpha - a).$$

Repetimos o processo substituindo a por a_1 obtendo um $a_2 \in K$ com

$$v(\alpha - a_2) > v(\alpha - a_1) > v(\alpha - a),$$

e após m passos $a_1, ..., a_m \in K$ com

$$v(\alpha - a_m) > ... > v(\alpha - a_1) > v(\alpha - a).$$

Como $(K, \mathcal{O})$ é finitamente ramificado, pelo Lema 3.6.14, existe apenas um número finito de valores entre 0 e $v(n)$, o que implica que após um número finito de repetições obtemos um $b \in K$ com

$$v(\alpha - b) > v(\alpha - a) + v(n). \tag{59}$$

Em particular,

$$v(a - b) = v((\alpha - b) - (\alpha - a)) = v(\alpha - a). \tag{60}$$

Finalmente temos

$$\begin{array}{lll} v(n)+v(a-b) & = v(n(a-b)) & = v(na-nb) \\ & \overset{(58)}{=} v\left(\sum_{i=1}^{n}\alpha_i - nb\right) & = v\left(\sum_{i=1}^{n}(\alpha_i - b)\right) \\ & \geq \min_{1\leq i\leq n}\{v(\alpha_i - b)\} & \overset{(57)}{=} v(\alpha - b) \\ & \overset{(59)}{>} v(\alpha - a) + v(n) & \overset{(60)}{=} v(a-b)+v(n), \end{array}$$

uma contradição. Donde concluímos que $K'|K$ não é extensão imediata própria, isto é, $K' = K$. Logo, K é algebricamente maximal.

■

Corolário 3.6.17 *Se $(K, \mathcal{O})$ é finitamente ramificada, então a Henselização de $(K, \mathcal{O})$ é caracterizada como a extensão algébrica maximal de $(K, \mathcal{O})$. (Ou seja, se $(K', \mathcal{O}')$ é uma extensão algébrica maximal de $(K, \mathcal{O})$, então ela é isomorfa à henselização de $(K, \mathcal{O})$.)*

Prova. Seja $(K', \mathcal{O}')$ uma extensão algebricamente maximal de $(K, \mathcal{O})$. A henselização de $(K', \mathcal{O}')$ é uma extensão algébrica imediata sua, e então, pela definição de extensão algebricamente maximal, o corpo $(K', \mathcal{O}')$ deve ser igual a sua henselização, e portanto $(K', \mathcal{O}')$ é Henseliano. Portanto a Henselização $(K'', \mathcal{O}'')$ de $(K, \mathcal{O})$ está contida em $(K', \mathcal{O}')$, pelo Teorema 3.6.9 (2).

Como, pelo Teorema 3.6.7, a Henselização $(K'', \mathcal{O}'')$ é uma extensão imediata de $(K, \mathcal{O})$ ela também é finitamente ramificada.

Logo, sendo $(K'', \mathcal{O}'')$ Henseliano e finitamente ramificada, temos, pelo Lema 3.6.14, que ela também é algebricamente maximal . Portanto $K'' = K'$.

■

4 Noções da Teoria de Modelos

De uma maneira bem simplificada e suficiente para este texto, a Teoria dos Modelos pode ser entendida como o estudo de *estruturas matemáticas*. No nosso caso, vamos considerar apenas sentenças da chamada *Lógica de primeira ordem*, que é simplesmante a lógica dos habituais cursos de matemática com apenas uma ressalva de caráter lógico que é importante ter-se em mente: quando fizermos uso do símbolo de quantificação "$\forall$" sempre estaremos quantificando a classe inteira à qual nos referimos. Assim, por exemplo, podemos quantificar sobre o conjunto dos números racionais $\mathbb{Q}$ quando estivermos nos referindo à teoria de corpos, mas não podemos, neste contexto, fazer o mesmo para o subconjunto $\mathbb{N}$ dos números naturais.

Dois são os métodos principais de estudo em Teoria de Modelos, a saber:

(I) Olhar para teorias que têm propriedades interessantes e provar teoremas gerais sobre os mode-los destas teorias, como, por exemplo, a teoria de corpos (de característica zero).

(II) Começar com uma estrutura matemática concreta, como o corpo dos números p-ádicos, e usar técnicas da Teoria de Modelos para obter novas informações sobre tal estrutura.

Desenvolvemos neste texto a abordagem (I), provando primeiro teoremas gerais da Teoria dos Modelos, e depois estudando estruturas concretas de nosso interesse, como os corpos valorizados.

Salientamos que as expressões citadas acima, tais como "modelo", "teoria" e "estrutura", parecem fazer certo sentido intuitivo, mas apenas para as nossas interpretações subjetivas. Do ponto de vista matemático, no entanto, devemos definí-las com precisão. De pronto então iniciamos tal tarefa.

Lembramos que tudo o que segue pressupõe conhecida a Teoria de Conjuntos. A referência para todo este capítulo é [11].

4.1 Construção de uma Linguagem Formal

Começamos pelo estudo do que pode ser chamado a parte *sintática* ou *gramatical* da linguagem, definindo um "alfabeto", ou seja, um conjunto de símbolos a partir do qual poderemos construir todas as "palavras", e por conseguinte "frases", de nosso interesse, e de tal modo que qualquer uma destas possam ser escritas como uma concatenação finita de tais símbolos.

- O alfabeto em uma linguagem formal de primeira ordem será constituído pelos seguintes símbolos:

  Símbolos lógicos : $\neg$ (negação) , $\wedge$ (e), $\forall$ (para todo), $\doteq$ (igual)
  Variáveis : $v_0, ..., v_n, ...$ $(n \in \mathbb{N})$
  Símbolos relacionais : R_i $(i \in I)$
  Símbolos funcionais : f_j $(j \in J)$
  Símbolos constantes : c_k $(k \in K)$
  Símbolos auxiliares : .) , (

Aqui, $\mathbb{N}$ é o conjunto dos números naturais e I, J e K são conjuntos quaisquer de índices (possivelmente iguais ao vazio).

- Denotaremos por Vbl o conjunto de todas as variáveis.

- Salientamos que pretendemos futuramente interpretar os símbolos R_i e f_j como relações e funções, mas no momento vamos encará-los de modo simbólico. Para isto, definimos funções dos conjuntos I e J com imagem nos números naturais que nos darão as "aridades" dos símbolos relacionais e funcionais respectivamente

$$\lambda : I \longrightarrow \mathbb{N} \qquad \mu : J \longrightarrow \mathbb{N}.$$

Note que, com isto, faz sentido definirmos as concatenações de símbolos

$$f_j(v_1, ..., v_{\mu(j)}) \quad \text{e} \quad R_i(v_1, ..., v_{\lambda(i)}),$$

por exemplo, pois podemos dizer a quantos parâmetros estamos aplicando o mesmo.

- Do ponto de vista de sintaxe podemos dizer que os símbolos e as funções aridades definidas acima nos dão as informações essencias da linguagem, e por isso definimos assinatura $\mathcal{L}$ da linguagem em questão pela tripla ordenada $\mathcal{L} = (\lambda, \mu, K)$, com λ e μ definidas como acima, e K sendo o conjunto de índices dos símbolos constantes. Pelos motivos mencionados acima, também chamaremos uma linguagem, a partir de agora, pelo nome de sua assinatura, ou seja, nos referiremos à linguagem $\mathcal{L}$.

- Estamos agora em uma posição bem mais confortável: uma linguagem $\mathcal{L}$ pode ser caracterizada como um objeto matemático concreto, a saber, uma tripla ordenada.

Definimos uma sobre-linguagem $\mathcal{L}'$ de uma linguagem de primeira ordem $\mathcal{L}$ como sendo uma linguagem $\mathcal{L}' = (\lambda', \mu', K')$ em que vale:

(1) $\lambda' : I' \longrightarrow \mathbb{N}$; $I \subset I'$ e $\lambda'(i) = \lambda(i)$ para todo $i \in I$.
(2) $\mu' : J' \longrightarrow \mathbb{N}$; $J \subset J'$ e $\mu'(j) = \mu(j)$ para todo $j \in J$.
(3) $K \subset K'$.

Salientamos o tipo de sobre-linguagem que será mais utilizada neste texto:

Definição 4.1.1 *Fixada uma linguagem de primeira ordem $\mathcal{L}$, denominamos linguagem ampliada por constantes , ou extensão por constantes, toda sobre-linguagem $\mathcal{L}' = (\lambda', \mu', K')$ que satisfizer $I = I'$, $J = J'$ e $K' = K \cup \underline{K}$ onde $K \cap \underline{K} = \emptyset$. Utilizamos neste caso as notações $\mathcal{L}_{\underline{K}}$ ou $\mathcal{L}(\underline{K})$.*

Assim, o conjunto $\underline{K}$ na definição acima atua como conjunto de índices para as novas constantes.

- Passamos agora à definição do que intuitivamente podemos considerar como as "palavras" da nossa linguagem. A partir de agora consideramos $\mathcal{L}$ uma linguagem fixada, e definimos inicialmente os termos da linguagem $\mathcal{L}$. Fazemos isto recursivamente.

Definição 4.1.2 *(Definição recursiva dos $\mathcal{L}$-termos)*

Fixada uma linguagem $\mathcal{L} = (\lambda, \mu, K)$, dizemos que:

(a) todas as variáveis v_n e todos os símbolos constantes c_k são $\mathcal{L}$-termos, para todo $n \in \mathbb{N}$ e todo $k \in K$;

(b) se $t_1, ..., t_{\mu(j)}$ são $\mathcal{L}$-termos, para algum $j \in J$, então $f_j(t_1, ..., t_{\mu(j)})$ é um $\mathcal{L}$-termo;

(c) Nenhuma outra seqüência de símbolos é um $\mathcal{L}$-termo.

Denotaremos o conjunto de todos os $\mathcal{L}$-termos por $Tm_{\mathcal{L}}$.

- Introduzimos agora as fórmulas da linguagem $\mathcal{L}$, que farão as vezes das "frases" na linguagem em questão.

Definição 4.1.3 *(Definição recursiva das $\mathcal{L}$-fórmulas)*

Fixada uma linguagem $\mathcal{L} = (\lambda, \mu, K)$, dizemos que:

(a) se t_1 e t_2 são $\mathcal{L}$-termos, então $(t_1 \doteq t_2)$ é uma $\mathcal{L}$-fórmula;

(b) se $t_1, ..., t_{\lambda(i)}$ são $\mathcal{L}$-termos, para algum $i \in I$, então $R_i(t_1, ..., t_{\lambda(i)})$ é uma $\mathcal{L}$-fórmula;

(c) se φ e ψ são $\mathcal{L}$-fórmulas e v é uma variável, então

$$\neg\varphi, \qquad (\varphi \wedge \psi) \qquad e \qquad \forall v\ \varphi$$

são $\mathcal{L}$-fórmulas;

(d) nenhuma outra seqüência de símbolos é uma $\mathcal{L}$-fórmula.

As $\mathcal{L}$-fórmulas $(t_1 \doteq t_2)$ e $R_i(t_1, ..., t_{\lambda(i)})$ são as mais simples, no sentido de gerarem recursivamente as outras, e por isso são chamadas de atômicas ou primas. Também utilizaremos a notação $Fml_{\mathcal{L}}$ para denotar o conjunto de todas as $\mathcal{L}$-fórmulas.

- Quando a linguagem $\mathcal{L}$ estiver fixada, ou não for importante saber em qual linguagem trabalhamos, chamaremos as $\mathcal{L}$-fórmulas e $\mathcal{L}$-termos, simplesmante por fórmulas e termos.

  Faremos uso também de letras gregas, tais como α, β, γ.... para indicar fórmulas, assim como letras latinas minúsculas tais como x, y, z... para

variáveis e, para termos, letras latinas minúsculas tais como $t, t_1, t_2, ...$, como bem já utilizamos na definição de termos.

- Será útil falarmos de sub-fórmulas de uma fórmula, as quais entenderemos por serem uma sub-seqüência de seus símbolos que, sozinhos, formam uma fórmula segundo nossas regras de construção.

  Só pelo que foi definido acima, podemos escrever uma infinidade de $\mathcal{L}$-fórmulas: por exemplo,

$$((\forall v_1\ (v_2 \doteq v_1)) \wedge \neg(v_1 \doteq v_2)) \wedge (\forall v_3\ \forall v_2\ (v_1 \doteq v_2 \doteq v_3))$$

  sendo $\forall v_1\ (v_2 \doteq v_1)$ uma de suas sub-fórmulas.

É conveniente, antes de prosseguirmos na sintaxe, dar exemplos do que especificamos até o momento:

Exemplo 4.1.4 *Neste texto, faremos uso das seguintes linguagens:*

1) A linguagem dos grupos abelianos totalmente ordenados: *Esta linguagem tem um símbolo funcional binário $+$, um símbolo relacional $<$, também binário e um símbolo constante 0. Desta forma, um exemplo de termo é*

$$((x_1 + 0) + (x_2 + x_3)) + x_4,$$

onde usamos simplificadamente $(t+t')$ para $+(t,t')$, para quaisquer termos t e t' da linguagem. E

$$((x < 0) \wedge ((x + y) \doteq 0)) \wedge (\neg(z < 0))$$

é um exemplo de fórmula desta linguagem, onde $(t < t')$ substitui $<(t,t')$, com t e t' termos.

2) A linguagem dos anéis e corpos: *Aqui fazemos uso de dois símbolos funcionais binários, $\cdot$ e $+$, e dois símbolos constantes, 0 e 1. Análogo ao que fizemos acima, usamos $(t.t')$ e $(t+t')$ no lugar de $\cdot(t+t')$ e $+(t+t')$, respectivamente, para t e t' termos desta linguagem. Um exemplo*

de termo para tal linguagem é

$$((1.x) + 0),$$

e de fórmula

$$(((1.x) + 0) \doteq x) \vee (\neg((1.x) \doteq (x + 0))).$$

3) A linguagem dos corpos valorizados: *Esta linguagem tem todos os símbolos da linguagem de corpos e um símbolo adicional V, unário, que caracteriza o anel de valorização que queremos considerar neste corpo. Assim, $V(a)$ significa que o elemento a pertence a este anel de valorização. Um exemplo de fórmula nesta linguagem é*

$$V(z) \wedge \exists y \ (yz \doteq 1 \wedge V(y))$$

que está expressando que z pertence ao anel de valorização e que é invertível aí.

Assim, fixado um anel de valorização, esta fórmula é utilizada para determinar as suas unidades.

- Para $\mathcal{L}$-fórmulas nem sempre é possível perguntar sobre o seu valor lógico. Por exemplo, na linguagem dos grupos abelianos totalmente ordenados, que possui um símbolo relacional binário $<$, a $\mathcal{L}$-fórmula $(0 < y)$ naturalmente não é adequada para questionarmos sobre seu valor lógico, ou seja, validade. De fato, só falaremos futuramente da validade de uma $\mathcal{L}$-fórmula se tal fórmula for de um tipo especial, mais precisamente, sem variáveis livres, quando então será chamada de $\mathcal{L}$-sentença. Passamos então a especificar o que significa uma $\mathcal{L}$-fórmula ter "variáveis livres". De maneira informal isto significa que existe uma variável na $\mathcal{L}$-fórmula em questão que não foi quantificada pelo símbolo $\forall$ [6].

[6]Veremos adiante (veja a Observação 4.1.12) que uma fórmula que envolve $\exists$ pode ser substituída por

Definição 4.1.5 *Dada uma fórmula escrita como $\forall v\ \varphi$, dizemos que φ é o alcance do quantificador $\forall v$. Uma ocorrência de uma variável v numa fórmula ψ é dita vinculada caso esta ocorrência caia no alcance de algum quantificador $\forall v$ que foi utilizado na construção de ψ. Caso contrário tal ocorrência é dita livre.*

Notação 4.1.6 *Denotamos por $Fr(\psi)$ o conjunto das variáveis que ocorrem livres em ψ.*

Pode-se verificar que valem as seguintes identidades para as fórmulas ψ e φ:

(a) $Fr(\psi) = \{v \mid v \text{ aparece em } \psi\}$, caso ψ é uma fórmula atômica.
(b) $Fr(\psi) = Fr(\neg\psi)$
(c) $Fr(\psi \wedge \varphi) = Fr(\psi) \cup Fr(\varphi)$
(d) $Fr(\forall x\ \varphi) = Fr(\varphi) \backslash \{x\}$.

Exemplo 4.1.7 *Na fórmula*

$$\forall x\ ((x \doteq y) \wedge (\forall y\ (\neg(y \doteq z) \wedge (x \doteq z))))$$

temos que a variável z é livre e que y e x não são livres, porém x é livre na sub-fórmula

$$\forall y\ (\neg(y \doteq z) \wedge (x \doteq z)).$$

Podemos agora definir formalmente:

Definição 4.1.8 *O conjunto das $\mathcal{L}$-sentenças denotado por $Sent_{\mathcal{L}}$ é definido por:*

$$Sent_{\mathcal{L}} = \{\varphi \in Fml_{\mathcal{L}} \mid Fr(\varphi) = \emptyset\}.$$

- Neste trabalho precisaremos ainda de uma operação sintática, chamada substituição de uma variável v em uma fórmula ζ por um $\mathcal{L}$-termo t. Primeiramente utilizamos a notação $\zeta(x_1, ...x_n)$ para indicar que $Fr(\zeta) = \{x_1, ..., x_n\}$.

outra que envolve $\forall$. e vice-versa.

Definição 4.1.9 *Definimos a substituição da variável v pelo termo t na fórmula φ como sendo a sequência de símbolos obtida pela substituição de cada ocorrência livre da variável v pelo termo t. Indicaremos tal substituição por*

$$\zeta(v/t).$$

Obviamente, quando não houver ocorrências livres de v em ζ, temos que $\zeta(v/t)$ é idêntica a ζ e que sempre $\zeta(v/v)$ é idêntica à ζ.

Se

$$Fr(\zeta) = \{x_1, ..., x_n\}$$

então, dados $t_1, ..., t_n$ termos, denotamos por $\zeta(x_1/t_1, ..., x_n/t_n)$ a substituição de x_i por t_i para cada $1 \leq i \leq n$ na fórmula ζ.

- Se v ocorre livre em uma fórmula φ que faz parte do alcance de um quantificador $\forall u$, e se a variável u ocorre em um termo t, então na substituição de v por t esta ocorrência da variável u obviamente cai no alcance de $\forall u$. Se isto não ocorrer para nenhuma variável de t, então dizemos que "t é livre de v em φ". Em outras palavras:

Definição 4.1.10 *Se t é um termo, v uma variável e φ uma fórmula, dizemos que t é livre de v em φ caso nenhuma ocorrência livre de v em φ caia no alcance de algum quantificador $\forall u$, o qual foi utilizado na consntrução de φ, e tal que u ocorra em t.*

Assim, se $u_1, ..., u_n$ são as únicas variáveis que aparecem em t, a variável v não pode estar no alcance dos quantificadores $\forall u_1, ..., \forall u_n$, caso estes apareçam na construção de φ.

Exemplo 4.1.11 *Na linguagem dos grupos abelianos totalmente ordenados consideramos a fórmula φ dada por*

$$v < 0 \quad \wedge \quad \forall u \; u < v \quad \vee \quad \forall y \; y < v + v$$

e os termos $(y+v)$, y, u, $(u+y)$, $(z+v)$, $(z+w)$ e z; onde $v, y, u, z, w \in Vbl$. Pela definição acima, os quatro primeiros termos ***não*** *são livres de de v em φ, enquanto os últimos três são livres de v em φ.*

Observamos também que sempre temos x livre de x em φ trivialmente.

Notação 4.1.12 *Para facilitar a escrita das fórmulas faremos uso de algumas abreviações e notações:*

1. $(\varphi \vee \psi)$ *no lugar de* $\neg(\neg\varphi \wedge \neg\psi)$. *(ou)*
2. $(\varphi \rightarrow \psi)$ *no lugar de* $\neg(\varphi \wedge \neg\psi)$. *(implica)*
3. $(\varphi \leftrightarrow \psi)$ *no lugar de* $(\neg(\varphi \wedge \neg\psi)) \wedge (\neg(\psi \wedge \neg\varphi))$. *(equivalente)*
4. $\exists v\ \varphi$ *no lugar de* $\neg(\forall v\ (\neg\varphi))$. *(existe)*
5. $t_1 \neq t_2$ *fica no lugar de* $\neg(t_1 \doteq t_2))$.
6. $t_1 R_i t_2$ *fica no lugar de* $R_i(t_1, t_2)$, *caso* $\lambda(i) = 2$.
7. $\forall u, v, w...$ *fica no lugar de* $\forall u \forall v \forall w....$
8. $\exists x, y...$ *fica no lugar de* $\exists x \exists y...$
9. $(\varphi_1 \wedge \varphi_2 \wedge \varphi_3)$ *substitui* $((\varphi_1 \wedge \varphi_2) \wedge \varphi_3)$, *ou seja, retiramos os parênteses.*
10. $(\varphi_1 \vee \varphi_2 \vee \varphi_3)$ *substitui* $((\varphi_1 \vee \varphi_2) \vee \varphi_3)$.
11. *Retiraremos das fórmulas outros parênteses, quando não houver chance de ambigüidades.*

Também escreveremos abreviadamente $\bigwedge_{i=1}^{n} \varphi_i$ *para uma conjunção finita*

$$(\varphi_1 \wedge ... \wedge \varphi_n)$$

e, analogamente, $\bigvee_{j=1}^{m} \psi_j$ *significa a disjunção finita*

$$(\psi_1 \vee ... \vee \psi_m).$$

Simbolizaremos por $\forall\varphi$ *a fórmula*

$$\forall\ x_1, ..., x_n\ \varphi(x_1, ..., x_n),$$

quando $Fr(\varphi) = \{x_1, .., x_n\}$.

Também usaremos as seguintes convenções lógicas habituais:

a. $\vee$ e $\wedge$ têm prioridade sobre $\rightarrow$ e $\leftrightarrow$.

b. $\neg$ têm prioridade sobre $\vee$ e $\wedge$.

Com estas convenções, a fórmula

$$\exists x \exists y((\neg(t_1 \doteq t_2)) \rightarrow ((\alpha \wedge \beta) \wedge \gamma))$$

reescreve-se simplesmente

$$\exists x, y((t_1 \neq t_2) \rightarrow \alpha \wedge \beta \wedge \gamma).$$

4.2 Elementos de Teoria da Prova

Nesta seção definiremos o que será para nós uma prova formal. O formalismo necessário para executar uma prova matemática é historicamente justificado pelos inúmeros paradoxos e mal-entendidos aos quais as provas puramente intuitivas podem nos levar. Na verdade, uma prova de algum fato matemático deve ser algo possível de ser verificado, pelo menos teoricamente, por qualquer pessoa, ou, quem sabe, um computador que "conheça" as regras de inferência. Assim, espera-se que uma prova seja constituída de um número finito de passos de inferência.

O que faremos então é listar as regras de inferência que utilizaremos, que nada mais são do que as regras utilizadas por qualquer matemático cotidianamente. Do que falamos acima, segue que uma prova em uma linguagem $\mathcal{L} = (\lambda, \mu, K)$ será uma sequência de $\mathcal{L}$-fórmulas obtidas a partir de regras de dedução, as quais, por sua vez, serão também definidas logo a seguir.

Definição 4.2.1 *Dado um conjunto não vazio $\Sigma \subset Fml_{\mathcal{L}}$, uma prova a partir de Σ na linguagem $\mathcal{L}$ é uma sequência finita $(\varphi_1, ..., \varphi_n)$ com $\varphi_i \in Fml_{\mathcal{L}}$ para $1 \leq i \leq n$, tal que:*

(1) $\varphi_i \in \Sigma$, *ou*

(2) φ_i *é um axioma lógico, ou*

(3) φ_i *é obtido pelo emprego de uma regra lógica a alguma outra fórmula* φ_j *já listada ou que se enquadra no caso* (1) *ou* (2), *para algum* $j \neq i$.

Precisamos agora dizer quais são os axiomas lógicos e as regras lógicas.

- Os axiomas lógicos são de três tipos:

1. Tautologias
2. Axiomas de quantificadores
3. Axiomas de identidade (lógica)

- Já como regras lógicas consideramos:

a. Modus Ponens

b. Regra da generalização.

A noção de axiomas lógicos e de regras lógicas é geral, no sentido de que independem da linguagem em estudo. Eles fazem parte da chamada *lógica de predicados.*

Para definir tautologia, precisamos de uma rápida incursão na linguagem da lógica de predicados. (Utilizaremos esta definição com detalhe no Teorema 4.4.13).

Nesta linguagem, consideramos o seguinte alfabeto:

$$) \ (\ \neg \ \wedge \ A_0, ..., A_n, ... \ \ (n \in \mathbb{N}),$$

onde os símbolos A_n, com $n \in \mathbb{N}$, são chamadas variáveis predicativas. Análogo à definição de fórmulas, definimos predicados (ou formas predicativas):

Definição 4.2.2

(*a*) $A_0, A_1, ...$ *são predicados.*

(*b*) *Se* φ *e* ψ *são predicados, então* $\neg\varphi$ *e* $(\varphi \wedge \psi)$ *são predicados.*

(*c*) *Nenhuma outra sequência de símbolos é um predicado.*

Faremos agora a primeira observação semântica (isto é, referente a significado) sobre predicados, a saber, uma observação referente a avaliação lógica das variáveis predicativas.

Definição 4.2.3 *Entendemos por uma avaliação lógica B das variáveis predicativas $A_0, A_1, \ldots$ uma aplicação do conjunto $\{A_0, A_1, \ldots\}$ no conjunto $\{V, F\}$ dos valores verdade tal que:*

(i) Para cada $n \in \mathbb{N}$ temos $B(A_n) = V$ ou $B(A_n) = F$.

(ii) $B(\neg\varphi) = -B(\varphi)$

(iii) $B((\varphi \wedge \psi)) = B(\varphi) \cap B(\psi)$, onde φ e ψ são predicados, e com $-$ e $\cap$ operações no conjunto $\{V, F\}$ definidas por

$\cap$	V	F
V	V	F
F	F	F

e

$-$	V	F
	F	V

Definição 4.2.4 *Um predicado φ é dito uma tautologia quando assume o valor V para toda avaliação B definida como acima.*

Salientamos que sempre podemos determinar se um predicado é uma tautologia ou não, pois temos no máximo 2^n avaliações para verificar, sendo n o número de variáveis predicativas. Por exemplo, para fórmulas $\varphi, \psi \in Fml_{\mathcal{L}}$, que são predicados, temos que $\neg((\varphi \wedge \psi) \wedge \neg\varphi)$ é uma tautologia. Podemos fazer, como de habitual, uma "tabela-verdade" para constatar tal fato.

φ	ψ	$\varphi \wedge \psi$	$\neg\varphi$	$(\varphi \wedge \psi) \wedge \neg\varphi$	$\neg((\varphi \wedge \psi) \wedge \neg\varphi)$
V	V	V	F	F	V
V	F	F	F	F	V
F	V	F	V	F	V
F	F	F	V	F	V

Para falarmos sobre os outros axiomas lógicos, voltamos para o nosso ponto de vista inicial (isto é, sem necessidade de falarmos em predicados). São eles:

Axioma 4.2.5 *Axiomas de quantificadores: Dados* $x \in Vbl$, $\varphi, \psi \in Fml_{\mathcal{L}}$ *e* $t \in Tm_{\mathcal{L}}$,

$(A1)$ $\forall x\ \varphi \to \varphi(x/t)$, *caso* t *é livre de* x *em* φ.

$(A2)$ $\forall x\ (\varphi \to \psi) \to (\varphi \to \forall x\ \psi)$, *caso* $x \notin Fr(\varphi)$.

Axioma 4.2.6 *Axiomas de identidades: Dados* $x, y, z, u, v \in Tm_{\mathcal{L}}$,

(I_1) $x \doteq x$.

(I_2) $x \doteq y \to (x \doteq z \to y \doteq z)$.

(I_3) $x \doteq y \to (R_i(v, ..., x, ..., u) \to R_i(v, ..., y, ..., u))$.

(I_4) $x \doteq y \to (f_j(v, ..., x, ..., u) \to f_j(v, ..., y, ..., u))$.

Resta-nos apenas enunciar as regras lógicas:

(MP) **Modus Ponens**: Se podemos escrever $\varphi \to \psi$ e φ, então podemos escrever ψ.

$(\forall)$ **Regra da generalização**: Se podemos escrever φ, então podemos escrever $\forall x\ \varphi$.

Com as regras lógicas acima estamos aceitando as concatenações do tipo

$$(.., \varphi \to \psi, ..., \varphi, ..., \psi, ...) \quad \text{e} \quad (..., \varphi, ..., \forall x\ \varphi, ...)$$

em uma prova.

Definição 4.2.7 *Dado um conjunto de fórmulas* Σ *de uma linguagem* $\mathcal{L}$, *dizemos que* φ *é* <u>dedutível de Σ</u> *caso exista uma prova de* φ *a partir das fórmulas pertencentes a* Σ.

Notação 4.2.8 *Escrevemos então*

$$\Sigma \vdash \varphi$$

para tal fato, e

$$\Sigma \nvdash \varphi$$

caso contrário.

As regras lógicas podem agora ser reescritas:

$$\begin{array}{l}\text{(MP) Modus Ponens : } \{(\varphi \to \psi), \varphi\} \vdash \psi. \\ (\forall) \text{ Regra da generalização : } \{\varphi\} \vdash \forall x\ \varphi\end{array} \tag{61}$$

e os axiomas

$$\begin{array}{l}(A_1)\ \{\forall x\ \varphi\} \vdash \varphi(x/t) \text{ para todo termo } t \text{ livre de } x \text{ em } \varphi. \\ (A_2)\ \{\forall x\ (\varphi \to \psi)\} \vdash (\varphi \to \forall x\ \psi) \text{ caso } x \notin Fr(\varphi).\end{array} \tag{62}$$

A partir dos axiomas, das tautologias e das regras (MP) e (∀) listados acima, é possível provar várias regras de dedução; porém nos limitamos aqui a listar, sem prova, aquelas que poderão vir a ser utilizadas neste texto. Os detalhes podem ser encontrados em [11].

$$\begin{array}{ll}\{(\varphi \wedge \psi)\} \vdash \varphi & (\wedge B_1) \\ \{(\varphi \wedge \psi)\} \vdash \psi & (\wedge B_2) \\ \{\varphi\} \vdash (\varphi \vee \psi) & (\vee B_1) \\ \{\psi\} \vdash (\varphi \vee \psi) & (\vee B_2) \\ \{(\varphi \to \psi)\} \vdash (\neg\psi \to \neg\varphi) & (CP) \\ \{(\varphi \leftrightarrow \psi)\} \vdash (\varphi \to \psi) & (\leftrightarrow B_1) \\ \{(\varphi \leftrightarrow \psi)\} \vdash (\psi \to \varphi) & (\leftrightarrow B_2) \\ \{(\varphi \to \psi), (\psi \to \sigma)\} \vdash (\varphi \to \sigma) & (IC) \\ \{\varphi, \psi\} \vdash (\varphi \wedge \psi) & (\wedge) \\ \{(\varphi \to \sigma), (\psi \to \sigma)\} \vdash ((\varphi \vee \psi) \to \sigma) & (\vee) \\ \{(t_1 \doteq t_2)\} \vdash ((t_2 \doteq t_1)) & (S) \\ \{(t_1 \doteq t_2), (t_2 \doteq t_3)\} \vdash (t_1 \doteq t_3) & (Tr) \\ \{(t \doteq t')\} \vdash (R_i(t_1, ..., t, ..., t_{\lambda(i)}) \to R_i(t_1, ..., t', ..., t_{\lambda(i)})) & (R_i) \\ \{(t \doteq t')\} \vdash (f_j(t_1, ..., t, ..., t_{\mu(j)}) \to f_j(t_1, ..., t', ..., t_{\mu(j)})) & (f_j)\end{array}$$

Chegamos ao ponto de enunciar o primeiro resultado do capítulo:

Lema 4.2.9 *Sejam $\varphi, \psi \in Fml_{\mathcal{L}}$ e $x \in Vbl$. Então:*

(a) $\Sigma \vdash \varphi$ *se e somente se* $\Sigma \vdash \forall x\ \varphi$

(*b*) $\Sigma \cup \{\psi\} \vdash \varphi$ *se e somente se* $\Sigma \cup \{\forall x\ \psi\} \vdash \varphi$

Prova. Relembramos inicialmente que a fórmula $\varphi(x/x)$ é idêntica à φ, e que sempre temos x livre de x em φ trivialmente.

(*a*) Se $(..., \varphi)$ é uma prova de φ a partir de Σ, então, usando a Regra de Generalização $(\forall)$, temos que $(..., \varphi\ ,\ \forall x\ \varphi)$ é uma prova de $\forall x\ \varphi$ a partir de Σ.

Reciprocamente, se $(..., \forall x\ \varphi)$ é uma prova de $\forall x\ \varphi$ a partir de Σ, então também temos, por (A_1) e pela observação acima, que $(..., \forall x\ \varphi, \varphi)$ é uma prova de φ a partir de Σ.

(*b*) Se $(\ ...\ ,\ \psi\ ,\ ...\ ,\ \varphi\ )$ é uma prova de φ a partir de $\Sigma \cup \{\psi\}$, então

$$(..., \forall x\ \psi, \psi, ..., \varphi)$$

é uma prova de φ a partir de $\Sigma \cup \{\forall x\ \psi, \psi\}$, a qual é uma prova a partir de $\Sigma \cup \{\forall x\ \psi\}$ por (A_1) e pela observação do início da prova.

Reciprocamente, se $(\ ...\ ,\ \forall x\ \psi\ ,\ ...\ ,\ \varphi\ )$ é uma prova de φ a partir de $\Sigma \cup \{\forall x\ \psi\}$, então

$$(...\ , \psi, \forall x\ \psi, ..., \varphi)$$

é uma prova de φ a partir de $\Sigma \cup \{\forall x\ \psi, \psi\}$, a qual, pela regra da generalização $(\forall)$, é uma prova a partir de $\Sigma \cup \{\psi\}$.

■

Empregando iteradamente o Lema 4.2.9(a), vê-se que a dedutibilidade de uma fórmula φ a partir de Σ é equivalente à dedutibilidade de $\forall\varphi$ (veja Notação 4.1.12).

Do mesmo modo, este lema nos diz que, se podemos deduzir uma fórmula de uma outra fórmula ψ, poderíamos ter feito isto já partindo de $\forall\psi$.

Sejam agora $\varphi, \psi \in Fml_{\mathcal{L}}$ e $\Sigma \subset Fml_{\mathcal{L}}$. Se vale $\Sigma \vdash (\varphi \to \psi)$, então obtemos imediatamente, com (MP), que $\Sigma \cup \{\varphi\} \vdash \psi$. Salientamos que nesta dedução não é relevante se φ contém variáveis livres ou não. No

entanto, para a recíproca necessitamos de $Fr(\varphi) = \emptyset$. Temos então um resultado que na prática é muito importante.

Teorema 4.2.10 *Sejam* $\Sigma \subset Fml_{\mathcal{L}}$, $\psi \in Fml_{\mathcal{L}}$ *e* $\varphi \in Sent_{\mathcal{L}}$. *Então, de* $\Sigma \cup \{\varphi\} \vdash \psi$, *obtém-se também* $\Sigma \vdash (\varphi \to \psi)$.

Prova. Mostramos por indução em n que se

$$(\varphi_1, ..., \varphi_n)$$

for uma prova de ψ (isto é, φ_n é idêntica a ψ) a partir de $\Sigma \cup \{\varphi\}$, então

$$(\varphi \to \varphi_1, ..., \varphi \to \varphi_n)$$

é uma prova de $\varphi \to \psi$, ou seja, uma prova de $\varphi \to \psi$ a partir de Σ.

Se $n = 1$, a prova é constituída apenas por φ_1 (que é então idêntico a ψ). Mas φ_1 ou é um axioma lógico ou é um elemento de Σ ou é a própria φ.

Caso 1 : φ_1 é um axioma lógico ou pertence a Σ. Neste caso, temos evidentemente

$$(\varphi_1, \varphi_1 \to (\varphi \to \varphi_1), \varphi \to \varphi_1),$$

onde aplicamos (MP) em φ_1 e na tautologia $\varphi_1 \to (\varphi \to \varphi_1)$. Temos assim uma prova de $\varphi \to \varphi_1$ a partir de Σ.

Caso 2 : φ_1 é idêntica a φ. Neste caso, a implicação $\varphi \to \varphi_1$ é uma tautologia , em particular uma prova de $\varphi \to \varphi_1$ a partir de Σ .

Para a passagem de indução, suponhamos que

$$(\varphi_1, ..., \varphi_n, \varphi_{n+1}) \tag{63}$$

é uma prova de ψ a partir de $\Sigma \cup \{\varphi\}$. Pela hipótese de indução,

$$(\varphi \to \varphi_1, ..., \varphi \to \varphi_n) \tag{64}$$

já é uma prova de $\varphi \to \varphi_n$ a partir de Σ, a qual pretendemos completar com $\varphi \to \varphi_{n+1}$ no seu final.

Caso 1 : φ_{n+1} (que é idêntico a ψ) é um axioma lógico ou pertence a Σ. Neste caso, aumentamos (64), utilizando o mesmo raciocínio feito para $n = 1$:

$$(\varphi \to \varphi_1, ..., \varphi \to \varphi_n, \varphi_{n+1}, \varphi_{n+1} \to (\varphi \to \varphi_{n+1}), \varphi \to \varphi_{n+1}),$$

obtendo assim uma prova de $\varphi \to \psi$ a partir de Σ.

Caso 2 : φ_{n+1} é identico a φ . Neste caso basta juntar a tautologia $\varphi \to \varphi_{n+1}$ ao fim da prova.

Agora, como $n+1 > 1$, existe a possibilidade de ter sido aplicado (MP) ou ($\forall$) em (63). Assim, existem aqui outros casos a serem considerados:

Caso 3 : φ_{n+1} foi obtida por (MP) em (63). Neste caso existem $i, j \leq n$, tal que a fórmula φ_j é da forma $\varphi_i \to \varphi_{n+1}$. Portanto, em (64) aparecem as fórmulas $\varphi \to \varphi_i$ e $\varphi \to (\varphi_i \to \varphi_{n+1})$. Então aumentamos (64) da seguinte forma

$$\begin{gathered}(..., (\varphi \to (\varphi_i \to \varphi_{n+1})) \to ((\varphi \to \varphi_i) \to (\varphi \to \varphi_{n+1})), \\ ..., (\varphi \to \varphi_i) \to (\varphi \to \varphi_{n+1}), \varphi \to \varphi_{n+1})\end{gathered}$$

sendo que a primeira fórmula adicionada é uma tautologia, e a outras duas foram obtidas por emprego de (MP). Obtemos assim uma prova de $\varphi \to \psi$ a partir de Σ.

Caso 4 : φ_{n+1} foi obtida com ($\forall$). Neste último caso existe um $i \leq n$, tal que φ_{n+1} é da forma $\forall x\ \varphi_i$ com x uma variável. A partir da fórmula $\varphi \to \varphi_i$ existente em (64), obtemos, pelo emprego de ($\forall$), a fórmula $\forall x\ (\varphi \to \varphi_i)$. Agora, , uma vez que, por hipótese, $Fr(\varphi) = \emptyset$, usando a regra ($CP\forall$) obtemos $\varphi \to \forall x\ \varphi_i$, que é idêntica a $\varphi \to \varphi_{n+1}$.

■

4.3 Completude da lógica de primeira ordem

Na seção anterior fizemos uma série de definições a fim de termos um conceito preciso de prova matemática.

Nesta seção, começamos a discutir o que precisa ocorrer para que uma sentença $\varphi \in Sent_{\mathcal{L}}$ não possa ser provada a partir de $\Sigma \subset Sent_{\mathcal{L}}$, ou seja, para que

$$\Sigma \nvdash \varphi.$$

Veremos que isto significa que podemos achar um "contra-exemplo", ou seja , uma "estrutura" na qual tal sentença não vale mas todas as de Σ valem. Com isto, estaremos também verificando a coerência da definição de prova, o que significa que se pudermos deduzir uma fórmula a partir de Σ, então ela valerá em toda estrutura em que são verdadeiras as sentenças de Σ.

Para provar todas as afirmações do parágrafo anterior necessitamos de uma preparação técnica. Embora as definições de estrutura e de validade de uma sentença sejam dadas somente no início da próxima seção, já conseguiremos construir aqui o desejado "contra-exemplo" para $\Sigma \nvdash \varphi$.

Primeiramente fazemos uma definição que será necessária como hipótese para tal construção.

Definição 4.3.1 *Dizemos que um conjunto $\Sigma \subset Sent_{\mathcal{L}}$ é não-contraditório caso não exista uma $\mathcal{L}$-sentença α, tal que*

$$\Sigma \vdash \alpha \quad \textit{e também} \quad \Sigma \vdash \neg\alpha.$$

Se um tal α existir, o conjunto Σ será chamado contraditório.

Observação 4.3.2 *Evidentemente, Σ é contraditório quando qualquer $\mathcal{L}$-sentença pode ser provada a partir de Σ. Reciprocamente, se Σ for contradiório, poderemos provar qualquer $\mathcal{L}$-sentença a partir de Σ. De fato, se este for o caso, então deve existir uma prova das $\mathcal{L}$-sentenças α e $\neg\alpha$ para algum α, e pela regra $(\wedge)$ existe uma prova de $(\alpha \wedge \neg\alpha)$ a partir de Σ. Da tautologia $(\alpha \wedge \neg\alpha) \rightarrow \beta$ e de (MP) temos a seguinte prova de β a partir de Σ:*

$$(..., \alpha, \neg\alpha, ..., (\alpha \wedge \neg\alpha), (\alpha \wedge \neg\alpha) \rightarrow \beta, ..., \beta)$$

Com esta observação provamos agora

Lema 4.3.3 *Seja* $\Sigma \subset Sent_{\mathcal{L}}$ *e* $\varphi \in Sent_{\mathcal{L}}$. *Então* $\Sigma \nvdash \varphi$ *equivale a* $\Sigma \cup \{\neg\varphi\}$ *ser não-contraditório.*

Prova. Vamos provar que $\Sigma \vdash \varphi$ equivale a $\Sigma \cup \{\neg\varphi\}$ ser contraditório.

Suponhamos que

$$\Sigma \vdash \varphi.$$

Mas então também vale

$$\Sigma \cup \{\neg\varphi\} \vdash \varphi;$$

por outro lado, é claro que

$$\Sigma \cup \{\neg\varphi\} \vdash \neg\varphi,$$

e portanto $\Sigma \cup \{\neg\varphi\}$ é contraditório.

Suponhamos agora que $\Sigma \cup \{\neg\varphi\}$ é contraditório. Então, pela observação acima, φ pode ser deduzida a partir de $\Sigma \cup \{\neg\varphi\}$:

$$\Sigma \cup \{\neg\varphi\} \vdash \varphi.$$

Com o Teorema da Dedução (Teorema 4.2.10), obtemos então

$$\Sigma \vdash (\neg\varphi \to \varphi)$$

Prolongamos agora a prova da fórmula $(\neg\varphi \to \varphi)$ a partir de Σ

$$(..., (\neg\varphi \to \varphi), (\neg\varphi \to \varphi) \to \varphi, \varphi),$$

A penúltima fórmula é uma tautologia e a última é obtida por (MP), assim $\Sigma \vdash \varphi$.

■

Com isto, um "contra-exemplo" para $\Sigma \vdash \varphi$ será um "domínio" no qual toda $\sigma \in \Sigma \cup \{\neg\varphi\}$ é verdadeira. Para constatar a coerência mencionada anteriormente, precisamos inicialmente construir, para qualquer conjunto

de sentenças não-contraditório Σ, um domínio no qual toda $\sigma \in \Sigma$ é verdadeira. Fazemos isto através de aumentos sistemáticos do conjunto não-contraditório Σ para conjuntos também não-contraditórios, construindo um domínio tão grande quanto for possível, e então verificando que este era o contra-exemplo que estavamos procurando. Fazemos isto em dois passos.

O primeiro passo é o mais técnico e mais difícil. A idéia é ampliarmos a linguagem em questão por constantes para que possamos fazer com que toda sentença existencial valha no domínio a ser construído. Daí, construímos um domínio para esta linguagem ampliada que satisfaz a seguinte propriedade: toda vez que uma "sentença existencial" valer neste domínio, sua validade poderá ser justificada por um exemplo, ou seja, existirá um símbolo constante c_k na linguagem ampliada tal que, quando substituímos a variável quantificada por c_k, obtemos uma sentença válida neste domínio.

Para isto estenderemos a linguagem original $\mathcal{L}$ por novas constantes. Mas primeiro precisamos do seguinte lema técnico.

Lema 4.3.4 *Sejam $\mathcal{L}^{(1)} \subset \mathcal{L}^{(2)}$ duas linguagens com $I^{(1)} = I^{(2)}$, $J^{(1)} = J^{(2)}$ e $K^{(1)} \cup \{0\} = K^{(2)}$, onde $0 \notin K^{(1)}$. Sejam $\varphi_1, ..., \varphi_n \in Sent_{\mathcal{L}^{(2)}}$ e seja y uma variável que não ocorre em nenhuma φ_i. Se*

$$(\varphi_1, ..., \varphi_n)$$

é uma prova em $\mathcal{L}^{(2)}$ de φ_n a partir do conjunto $\Sigma = \{\varphi_1, ..., \varphi_m\}$, sendo $m \leq n$, então

$$(\varphi_1(c_0/y), ..., \varphi_n(c_0/y))$$

é uma prova em $\mathcal{L}^{(1)}$ de $\varphi_n(c_0/y)$ a partir do conjunto

$$\{\varphi_1(c_0/y), ..., \varphi_m(c_0/y)\},$$

onde c_0 é o novo símbolo constante introduzido em $\mathcal{L}^{(2)}$.

Prova. Inicialmente observamos que se φ_i é uma tautologia ou axioma de identidade então $\varphi_i(c_0/y)$ o continua sendo. Queremos mostrar que o

mesmo acontece quando φ_i é um dos axiomas de quantificadores.

Se φ_i é da forma (A1), ou seja,

$$\forall x\ \psi \rightarrow \psi(x/t),$$

onde t é livre de x em ψ, observamos que, para um y que não ocorre em φ_i, como t é livre de x em ψ, temos também que $t(c_0/y)$ é livre de x em ψ, e portanto vale:

$$\psi(x/t)(c_0/y) \quad \text{é idêntica a} \quad \psi(c_0/y)(x/t(c_0/y)).$$

Basta observarmos que, pelas substituições em ψ e t, chegamos em $\psi(y, t(y))$, uma vez que ψ envolve possivelmente c_0 e x, e t envolve possivelmente c_0.

Com isto $\varphi_i(c_0/y)$ é também da forma de axioma do tipo (A1), a saber

$$\forall x\ \psi(c_0/y) \rightarrow \psi(c_0/y)(x/t(c_0/y)).$$

No caso em que φ_i é da forma (A2), basta utilizar o resultado obtido para (A1) e observar que obtemos novamente um axioma do tipo (A2).

Seguimos agora por indução em n.

Se $n = 1$ e $m = 0$ (ou seja $\Sigma = \emptyset$), então φ_1 deve ser um axioma lógico. Como visto acima, $\varphi_1(c_0/y)$ é também um axioma lógico, e portanto

$$(\varphi_1(c_0/y))$$

é uma prova de $\varphi_1(c_0/y)$ a partir de $\Sigma = \emptyset$.

Se $n = 1$ e $m = 1$, ou φ_1 é um axioma lógico ou $\varphi_1 \in \Sigma$. O primeiro caso já foi considerado acima, e o segundo caso é claro.

Sejam agora $n \geq 2$ e

$$(\varphi_1, ..., \varphi_n)$$

uma prova em $\mathcal{L}^{(2)}$ a partir do conjunto $\Sigma = \{\varphi_1, ..., \varphi_m\}$, sendo $m \leq n$.

Se $m = n$ então $\varphi_n \in \Sigma$ e, pelo suposto acima, claramente

$$(\varphi_1, ..., \varphi_{n-1})$$

é uma prova de φ_{n-1} em $\mathcal{L}^{(2)}$ a partir do conjunto $\{\varphi_1, ..., \varphi_{n-1}\}$. Pela hipótese de indução,

$$(\varphi_1(c_0/y), ..., \varphi_{n-1}(c_0/y))$$

é uma prova de $\varphi_{n-1}(c_0/y)$ em $\mathcal{L}^{(1)}$ a partir de

$$\{\varphi_1(c_0/y), ..., \varphi_{n-1}(c_0/y)\}.$$

Portanto,

$$(\varphi_1(c_0/y), ..., \varphi_{n-1}(c_0/y), \varphi_n(c_0/y))$$

é uma prova de $\varphi_n(c_0/y)$ em $\mathcal{L}^{(1)}$ a partir de

$$\{\varphi_1(c_0/y), ..., \varphi_{n-1}(c_0/y), \varphi_n(c_0/y)\}.$$

Se $m < n$ então $m \leq n - 1$. Daí:

- Se φ_n é um axioma lógico então $\varphi_n(c_0/y)$ é também um axioma lógico e

$$(\varphi_1, ..., \varphi_{n-1})$$

é uma prova de φ_{n-1} em $\mathcal{L}^{(2)}$ a partir do conjunto $\{\varphi_1, ..., \varphi_m\}$. Pela hipótese de indução,

$$(\varphi_1(c_0/y), ..., \varphi_{n-1}(c_0/y))$$

é uma prova de $\varphi_{n-1}(c_0/y)$ em $\mathcal{L}^{(1)}$ a partir de

$$\{\varphi_1(c_0/y), ..., \varphi_m(c_0/y)\}.$$

Portanto, como $\varphi_n(c_0/y)$ é um axioma lógico,

$$(\varphi_1(c_0/y), ..., \varphi_{n-1}(c_0/y), \varphi_n(c_0/y))$$

é uma prova de $\varphi_n(c_0/y)$ em $\mathcal{L}^{(1)}$ a partir de

$$\{\varphi_1(c_0/y), ..., \varphi_m(c_0/y)\}.$$

- Se $\varphi_n \in \Sigma$, repetimos o argumento utilizado no caso $m = n$.

Faltam então dois casos, os quais se referem à situação em que φ_n é obtido pelo emprego de alguma regra lógica (veja 61).

- Se φ_n é obtido pela regra lógica (MP): Neste caso existem $i, j \leq n-1$, tal que φ_j tem a forma $(\varphi_i \to \varphi_n)$. Então $\varphi_j(c_0/y)$ tem a forma

$$\varphi_i(c_0/y) \to \varphi_n(c_0/y).$$

Assim obtemos $\varphi_n(c_0/y)$ por (MP).

- Se φ_n é obtido pela regra lógica $(\forall)$: Neste caso existe um $i \leq n-1$, tal que φ_n tem a forma $\forall x\ \varphi_i$. Então $\varphi_n(c_0/y)$ tem a forma $\forall x\ \varphi_i(c_0/y)$. Assim $\varphi_n(c_0/y)$ também é obtida de $(\forall)$.

■

Teorema 4.3.5 *Seja Σ um subconjunto não-contraditório de $Sent_{\mathcal{L}}$. Então existe uma linguagem $\mathcal{L}' \supset \mathcal{L}$ com $I' = I$, $J' = J$ e existe um subconjunto não-contraditório Σ' de $Sent_{\mathcal{L}'}$, com $\Sigma \subset \Sigma'$ e tal que, se*

$$\exists x\ \varphi$$

é uma $\mathcal{L}'$-sentença então existe $k \in K'$ tal que

$$(\exists x\ \varphi \to \varphi(x/c_k)) \in \Sigma'.$$

Prova. Construiremos a linguagem ampliada por constantes $\mathcal{L}'$ através de um processo enumerável, construindo, para cada $n \in \mathbb{N}$, uma linguagem $\mathcal{L}_n$, o que, por sua vez, é feito de maneira recursiva:

(1) $\mathcal{L}_0 = \mathcal{L}$;

(2) Se, para $n > 0$, $\mathcal{L}_{n-1} = (I_{n-1}, J_{n-1}, K_{n-1})$, então

$$\mathcal{L}_n = (I_{n-1}, J_{n-1}, K_{n-1} \cup \underline{K_{n-1}}),$$

onde $\underline{K_{n-1}}$ é um conjunto disjunto de K_{n-1}, de tal maneira, que existe uma bijeção

$$g_n : \underline{K_{n-1}} \to \{\exists x\ \varphi \mid \exists x\ \varphi \in Sent_{\mathcal{L}_{n-1}}\}$$

de $\underline{K_{n-1}}$ sobre o conjunto das sentenças existenciais da linguagem $\mathcal{L}_{n-1}$.

Assim, estamos contando todas as sentenças existenciais de $\mathcal{L}_{n-1}$ e denotando-as com novos índices de maneira inequívoca. Salientamos que os conjuntos $\underline{K_{n-1}}$ e as bijeções g_n existem sempre, pois todo conjunto possui alguma cardinalidade.

Obtemos assim uma cadeia ascendente de linguagens

$$\mathcal{L}_0 \subset \mathcal{L}_1 \subset ... \subset \mathcal{L}_{n-1} \subset \mathcal{L}_n \subset ...$$

Finalmente, definimos

$$\mathcal{L}' = \bigcup_{n\in\mathbb{N}} \mathcal{L}_n,$$

ou seja

$$I' = I, \quad J' = J \quad \text{e} \quad K' = \bigcup_{n\in\mathbb{N}} K_n,$$

onde, para cada $n \in \mathbb{N}\backslash\{0\}$,

$$K_n = K_{n-1} \cup \underline{K_{n-1}}.$$

Daí conclui-se, imediatamente, que também vale

$$Sent_{\mathcal{L}'} = \bigcup_{n\in\mathbb{N}} Sent_{\mathcal{L}_n}.$$

Assim, se $\exists x\ \varphi$ é uma $\mathcal{L}'$-sentença, então ela está no conjunto $Sent_{\mathcal{L}_{n-1}}$ para algum $n \in \mathbb{N}$. Daí, se definirmos o conjunto de sentenças Σ' do mesmo

modo, a saber, como uma união de uma cadeia ascendente

$$\Sigma = \Sigma_0 \subset \Sigma_1 \subset ... \subset \Sigma_{n-1} \subset \Sigma_n \subset ...;$$

construída de tal forma que, para tal φ existem um n e um $k \in \underline{K_{n-1}}$ tais que

$$(\exists x\ \varphi \rightarrow \varphi(x/c_k)) \in \Sigma_n,$$

restará apenas mostrar que

$$\Sigma' = \bigcup_{n \in \mathbb{N}} \Sigma_n$$

é não-contraditório.

Para isto, definimos:

$$\Sigma_n := \Sigma_{n-1} \cup \{(\exists x\ \varphi \rightarrow \varphi(x/c_k)) \mid k \in \underline{K_{n-1}}\ ,\ g_n(k) = \exists x\ \varphi\}.$$

Pela sobrejetividade de g_n cada sentença existencial $\exists x\ \varphi$ em $\mathcal{L}_{n-1}$ é atingida por alguma constante $k \in \underline{K_{n-1}}$:

$$g_n(k) = \exists x\ \varphi.$$

Como $Fr(\varphi) \subset \{x\}$, temos que $\varphi(x/c_k)$ é novamente uma sentença. Assim, vale $\Sigma_n \subset Sent_{\mathcal{L}_n}$. Agora mostramos a propriedade mais importante de Σ_n que é a de ser não-contraditório, o que fazemos a seguir por indução em n.

Para $n = 0$, $\Sigma_0 = \Sigma$ é não-contraditório por hipótese.

Suponhamos que existe $n \geq 1$ tal que Σ_{n-1} é não-contraditório mas Σ_n o é. Existe então uma sentença $\alpha \in Sent_{\mathcal{L}'}$ tal que

$$\Sigma_n \vdash (\alpha \wedge \neg\alpha)$$

Como toda prova de Σ_n utiliza apenas um número finito de axiomas de Σ_n , temos que $(\alpha \wedge \neg\alpha)$ é dedutível de Σ_{n-1} juntamente com um número

finito de sentenças, digamos,

$$\exists x_1\ \varphi_1 \to \varphi_1(x_1/c_{k_1}),\quad \ldots\quad ,\quad \exists x_r\ \varphi_r \to \varphi_r(x_r/c_{k_r}),$$

onde $g_n(k_i) = \exists x_i\ \varphi_i \in Sent_{\mathcal{L}_{n-1}}$ para $1 \leq i \leq r$, e que denotaremos resumidamente por $\sigma_1, ..., \sigma_r$. Ou seja:

$$\Sigma_{n-1} \cup \{\sigma_1, ..., \sigma_r\} \vdash (\alpha \wedge \neg\alpha).$$

Podemos, além disto, assegurar que uma prova de $(\alpha \wedge \neg\alpha)$ já existe na sub-linguagem $\mathcal{L}^{(2)}$ de $\mathcal{L}_n$ construída da seguinte maneira:

$$I^{(2)} = I_n,\quad J^{(2)} = J_n \quad \text{e} \quad K^{(2)} = K_{n-1} \cup \{k_1, ..., k_r\}.$$

Com o Teorema 4.2.10, obtemos

$$\Sigma_{n-1} \cup \{\sigma_2, ..., \sigma_r\} \vdash (\sigma_1 \to (\alpha \wedge \neg\alpha)),$$

e, pela utilização da tautologia

$$((\beta \to \gamma) \to (\alpha \wedge \neg\alpha)) \to (\beta \wedge \neg\gamma),$$

e por (MP), segue finalmente que

$$\Sigma_{n-1} \cup \{\sigma_2, ..., \sigma_r\} \vdash (\exists x_1\ \varphi_1 \wedge \neg\varphi_1(x_1/c_{k_1})). \tag{65}$$

Considerando que $\exists x_1$ é uma abreviação para $\neg\forall x_1\neg$, obtemos com a regra $(\wedge B_1)$, por um lado

$$\Sigma_{n-1} \cup \{\sigma_2, ..., \sigma_r\} \vdash \neg\forall x_1\ \neg\varphi_1 \tag{66}$$

e, por outro lado, com $(\wedge B_2)$ aplicado a (65),

$$\Sigma_{n-1} \cup \{\sigma_2, ..., \sigma_r\} \vdash \neg\varphi_1(x_1/c_{k_1}). \tag{67}$$

As dedutibilidades em (66) e (67) estão "escritas" na sub-linguagem $\mathcal{L}^{(2)}$ de $\mathcal{L}_n$. Definindo agora a sub-lingugagem $\mathcal{L}^{(1)}$ através de $I^{(1)} = I_n$,

$J^{(1)} = J_n$ e $K^{(1)} = K_{n-1} \cup \{k_2, ..., k_r\}$, vemos que $\neg\forall x_1\ \neg\varphi_1$, bem como o conjunto

$$\Pi = \Sigma_{n-1} \cup \{\sigma_2, ..., \sigma_r\}$$

já pertence a $Sent_{\mathcal{L}^{(1)}}$. Empregando agora o Lema 4.3.4 sobre a dedutibilidade (66) e (67), obtemos as seguintes dedutibilidades em $\mathcal{L}^{(1)}$,

$$\begin{aligned} &\Pi \vdash \neg\forall x_1\ \neg\varphi_1, \\ &\Pi \vdash \neg\varphi_1(x_1/c_{k_1})(c_{k_1}/y), \end{aligned} \tag{68}$$

sendo y uma "nova" variável, ou seja , a qual não aparece na prova de $\neg\varphi_1(x_1/c_{k_1})$ a partir de Π. Como

$$\varphi_1(x_1/c_{k_1})(c_{k_1}/y) = \varphi_1(x_1/y),$$

com $\varphi_1 \in Fml_{\mathcal{L}_{n-1}}$ vale sempre, temos

$$\Pi \vdash \neg\varphi_1(x_1/y).$$

Através do emprego de $(\forall)$ sobre y obtemos

$$\Pi \vdash \forall y\ \neg\varphi_1(x_1/y)$$

e, por (A_1),

$$\Pi \vdash \neg\varphi_1(x_1/y)(y/x_1).$$

Note que y é nova variável em φ_1, e então reconhecemos a identidade

$$\varphi_1(x_1/y)(y/x_1) = \varphi_1.$$

Temos assim

$$\Pi \vdash \neg\varphi_1,$$

e com isto finalmente obtemos de $(\forall)$

$$\Pi \vdash \forall x_1\ \neg\varphi_1.$$

Esta dedutibilidade, junto com (68)

$$\Pi \vdash \neg\forall x_1 \neg\varphi_1,$$

mostra que Π é contraditório em $\mathcal{L}^{(1)}$. Note que a prova acima foi feita na linguagem $\mathcal{L}_{n-1}$ com as constantes adicionais $c_{k_2}, .., c_{k_r}$, e que $\varphi_1 \in Fml_{\mathcal{L}_{n-1}(\{k_2,...,k_r\})}$.

Mostramos assim que, se $\Sigma_{n-1} \cup \{\sigma_1, ..., \sigma_r\}$ for contraditório então, $\Sigma_{n-1} \cup \{\sigma_2, ..., \sigma_r\}$ será contraditório em $\mathcal{L}_{n-1}(\{k_2, ..., k_r\})$. Logo, por iterações, podemos mostrar que Σ_{n-1} já era contraditório em $\mathcal{L}_{n-1}$, pelas observações acima. Esta contradição, junto com nossa hipótese de Σ_{n-1} ser não-contraditório, prova que Σ_n é não-contraditório. Concluímos que todos os Σ_n são não-contraditórios. Afirmamos que então $\Sigma' = \bigcup_{n\in\mathbb{N}} \Sigma_n$ é não-contraditório.

De fato, a prova de uma contradição a partir de Σ' é uma seqüência finita de fórmulas e tanto a linguagem $\mathcal{L}$ quanto o conjunto Σ' são construídos a partir de uma cadeia ascendente; por isso, existe $n \in \mathbb{N}$ tal que esta prova já está na linguagem $\mathcal{L}_n$ e provém de Σ_n. No entanto, isto é impossível pela já sabida não-contraditoriedade de Σ_n em $\mathcal{L}_n$.

■

Passamos agora a provar, via Lema de Zorn, a existência de um conjunto maximal de sentenças não contraditório para, a seguir, construir o domínio que procuramos.

Teorema 4.3.6 *Para cada conjunto não-contraditório $\Sigma \subset Sent_{\mathcal{L}}$ existe um sobreconjunto maximal $\Sigma^* \subset Sent_{\mathcal{L}}$ de Σ tal que Σ^* é não-contraditório. Ou seja, $\Sigma \subset \Sigma^* \subset Sent_{\mathcal{L}}$ e, caso $\Sigma^* \subset \Sigma_1 \subset Sent_{\mathcal{L}}$ e Σ_1 é não contraditório, então $\Sigma^* = \Sigma_1$.*

Prova. Consideremos o sistema

$$M = \{\Sigma_1 \subset Sent_{\mathcal{L}} \mid \Sigma \subset \Sigma_1 \ , \ \Sigma_1 \text{ é não-contraditório}\},$$

parcialmente ordenado pela inclusão.

Como $\Sigma \in M$, temos que M não é vazio. Seja $M' \subset M$ um subsistema totalmente ordenado pela inclusão; então pela demonstração acima, o conjunto

$$\Sigma' = \bigcup_{\Sigma_1 \in M'} \Sigma_1$$

é não-contraditório, e portanto pertence a M, e é, evidentemente, uma cota superior para M' em M .

Com isto nós mostramos que o sistema M satisfaz as hipóteses do Lema de Zorn. Assim, existe um elemento maximal Σ^* em M. Pela definição de M, $\Sigma \subset \Sigma^*$ e Σ^* é não-contraditório.

■

Aplicando agora o Teorema 4.3.6 ao conjunto $\Sigma' \subset Sent_{\mathcal{L}'}$ obtido no Teorema 4.3.5, obtemos um sobreconjunto $\Sigma^* \subset Sent_{\mathcal{L}'}$ maximal e não-contraditório de Σ'. Para tal Σ^* vale portanto:

$$\begin{aligned} &\text{(I) } \Sigma^* \subset Sent_{\mathcal{L}'} \text{ é não-contraditório maximal} \\ &\text{(II) Para cada } \exists x\, \varphi \in Sent_{\mathcal{L}'} \text{ existe um } k \in K' \text{ com} \\ &(\exists x\, \varphi \to \varphi(x/c_k)) \in \Sigma^*. \end{aligned} \tag{69}$$

Mostramos a seguir que estas propriedades de Σ^* nos levam canonicamente a um domínio e, na próxima seção, após definirmos "validade", mostramos que nele toda sentença $\sigma \in \Sigma^*$ é válida.

Para a construção deste domínio, consideramos inicialmente o conjunto dos $\mathcal{L}'$-termos constantes

$$TC = \{t \in Tm_{\mathcal{L}'} \mid \text{nenhuma variável aparece em } t\}. \tag{70}$$

Em particular todo c_k com $k \in K'$ pertence a TC. Definimos sobre TC a seguinte relação binária: se $t_1, t_2 \in TC$ então

$$t_1 \approx t_2 \quad \text{se e só se} \quad \Sigma^* \vdash (t_1 \doteq t_2). \tag{71}$$

Com o emprego do axioma (I_1) e das regras (S) e (Tr) é fácil ver que $\approx$ é uma relação de equivalência. O domínio que procuramos é o conjunto de todas as classes de equivalência:

$$A = TC/\approx . \tag{72}$$

Denotaremos as classes de equivalência por $\bar{t}$, e portanto

$$\bar{t} = \{t_1 \in TC \mid t \approx t_1\} \quad \text{e} \quad \overline{t_1} = \overline{t_2} \quad \text{se e só se} \quad t_1 \approx t_2. \tag{73}$$

Finalmente, para podermos falar de "validade" em tal donínio, precisamos dar interpretações para os símbolos R_i,f_j e c_k da linguagem $\mathcal{L}'$

- Para cada $i \in I$ definimos uma $\lambda(i)$-ária relação $\mathfrak{R}_i$ no domínio A, por

$$\mathfrak{R}_i(\overline{t_1}, ..., \overline{t_{\lambda(i)}}) \quad \text{se e só se} \quad \Sigma^* \vdash R_i(t_1, ..., t_{\lambda(i)}) \tag{74}$$

  para $\overline{t_1}, ..., \overline{t_n}$ fixados.

Afirmamos que esta definição independe dos representantes das classes, ou seja, se

$$t_1 \approx {t_1}', ..., t_{\lambda(i)} \approx t'_{\lambda(i)},$$

então

$$\Sigma^* \vdash R_i(t_1, ..., t_{\lambda(i)}) \quad \text{se e só se} \quad \Sigma^* \vdash R_i({t_1}', ..., t'_{\lambda(i)})$$

De fato, por simetria basta provar uma direção. Suponhamos então que

$$\Sigma^* \vdash R_i(t_1, ..., t_{\lambda(i)}).$$

Pela definição da relação $\approx$, temos que $\Sigma^* \vdash (t_\nu \doteq t'_\nu)$ para todo $1 \leq \nu \leq \lambda(i)$. Com isto, a prova que obtemos, a partir de Σ^*,

$$(..., (t_1 \doteq t'_1), ..., (t_{\lambda(i)} \doteq t'_{\lambda(i)}), R_i(t_1, ..., t_{\lambda(i)}))$$

pode ser continuada da seguinte forma:

$$(..., R_i(t_1, ..., t_{\lambda(i)}), R_i(t_1, ..., t_{\lambda(i)}) \to R_i(t'_1, ..., t_{\lambda(i)}), R_i(t'_1, ..., t_{\lambda(i)}), \\ ..., R_i(t'_1, ..., t'_{\lambda(i)})),$$

onde utilizamos intercaladamente a regra (R_i) e (MP). Portanto,

$$\Sigma^* \vdash R_i(t'_1, ..., t'_{\lambda(i)}).$$

- Para cada $j \in J$ definimos uma $\mu(j)$-ária função $\mathfrak{f}_j$ sobre o domínio A da seguinte forma: dadas as classes $\overline{t_1}, ..., \overline{t_{\mu(j)}}$,

$$\mathfrak{f}_j(\overline{t_1}, ..., \overline{t_{\mu(j)}}) := \overline{f_j(t_1, ..., t_{\mu(j)})}. \tag{75}$$

A independência da escolha das classses nesta definição, pode ser obtida da mesma maneira que acima, só que desta vez usando as regras (f_j) e (Tr), juntamente com a definição de equivalência de termos, mostrando com isso que

$$f_j(t_1, ..., t_{\mu(j)}) \doteq f_j(t'_1, ..., t'_{\mu(j)}).$$

- Por fim, para cada $k \in K$ nós definimos

$$\overline{c_k} \text{ como a interpretação de } c_k \text{ em } TC/\approx . \tag{76}$$

Nosso objetivo, a partir daqui, é mostrar que, com estas interpretações, todas as sentenças $\sigma \in \Sigma^*$ (e apenas estas) valem no domínio A. Mas isto só ficará definitivamente esclarecido depois que apresentarmos o conceito de validade, o que fazemos na próxima seção. Encerramos esta seção provando mais dois resultados técnicos que nos ajudarão a atingir este objetivo.

Definição 4.3.7 *Um conjunto de $\mathcal{L}-$sentenças Σ não-contraditório é dito dedutivamente fechado se, para cada $\alpha \in Sent_{\mathcal{L}}$ se $\Sigma \vdash \alpha$ então $\alpha \in \Sigma$.*

Lema 4.3.8 *Todo conjunto não-contraditório maximal de sentenças Σ^* é dedutivamente fechado.*

Prova. Por ser Σ^* não-contraditório maximal, basta provar que $\Sigma^* \cup \{\alpha\}$ é não-contraditório, se $\Sigma^* \vdash \alpha$. Isto porém é claro: se $\Sigma^* \cup \{\alpha\}$ fosse contraditório , em particular teríamos

$$\Sigma^* \cup \{\alpha\} \vdash \neg\alpha,$$

o que, pelo Teorema 4.2.10, nos levaria a

$$\Sigma^* \vdash (\alpha \rightarrow \neg\alpha).$$

Pela tautologia

$$(\alpha \rightarrow \neg\alpha) \rightarrow \neg\alpha$$

teríamos finalmente

$$\Sigma^* \vdash \neg\alpha,$$

e portanto Σ^* seria contraditório, absurdo.

■

Teorema 4.3.9 *Se um conjunto $\Sigma^* \subset Sent_{\mathcal{L}'}$ tem as propriedades (I) e (II) de (69) então, para todos $\alpha, \beta, \forall x\ \varphi \in Sent_{\mathcal{L}'}$:*

(a) $\neg\alpha \in \Sigma^*$ *se e só se* $\alpha \notin \Sigma^*$
(b) $(\alpha \wedge \beta) \in \Sigma^*$ *se e só se* $(\alpha \in \Sigma^*$ *e* $\beta \in \Sigma^*)$.
(c) $\forall\ x\ \varphi \in \Sigma^*$ *se e só se* $\varphi(x/t) \in \Sigma^*$ *para todo* $t \in TC$,

onde TC é o conjunto dos termos constantes de $\mathcal{L}'$.

Prova. (a) Como Σ^* é não-contraditório, não pode ocorrer de ambos α e $\neg\alpha$ pertencerem a Σ^*. Falta provar que $\neg\alpha \in \Sigma^*$, caso $\alpha \notin \Sigma^*$. De $\alpha \notin \Sigma^*$ obtemos imediatamente do Lema 4.3.8 que $\Sigma^* \nvdash \alpha$. Daqui, segue com o Lema 4.3.3, que $\Sigma^* \cup \{\neg\alpha\}$ é não contraditório. Porém Σ^* é maximal não contraditório, donde segue que $\Sigma^* \cup \{\neg\alpha\} = \Sigma^*$, ou seja, $\neg\alpha \in \Sigma^*$.

(b) De $(\alpha \wedge \beta) \in \Sigma^*$ segue trivialmente que $\Sigma^* \vdash (\alpha \wedge \beta)$ e por isto, com o uso das regras $(\wedge B_1)$ e $(\wedge B_2)$, então $\Sigma^* \vdash \alpha$ e $\Sigma^* \vdash \beta$. Pelo Lema 4.3.8, $\alpha \in \Sigma^*$ e $\beta \in \Sigma^*$. A recíproca mostra-se com a regra $(\wedge)$.

(*c*) Se $\forall x\ \varphi \in \Sigma^*$, então segue $\Sigma^* \vdash \forall x\ \varphi$ e com a regra $(\forall B)$ obtemos $\Sigma^* \vdash \varphi(x/t)$, caso $t \in TC$. (Observe que cada termo constante é livre de qualquer variável em φ). Com o Lema 4.3.8 obtemos novamente $\varphi(x/t) \in \Sigma^*$. Falta então mostrar a recíproca.

Suponhamos que $\forall x\ \varphi$ não está em Σ^*. Então, por *(a)*,

$$\neg\forall x\ \varphi \in \Sigma^*.$$

Agora queremos concluir que $\exists x\ \neg\varphi \in \Sigma^*$. Com a tautologia $(\neg\neg\varphi \to \varphi)$ obtemos que $\Sigma^* \vdash (\neg\neg\varphi \to \varphi)$.

Daí segue do Lema 4.2.9 que $\Sigma^* \cup \{\neg\neg\varphi\} \vdash \varphi$ e novamente pelas partes (a) e (b) do mesmo lema,

$$\Sigma^* \cup \{\forall x\ \neg\neg\varphi\} \vdash \forall x\ \varphi.$$

A hipótese $\forall x\ \varphi \in Sent_{\mathcal{L}'}$ implica que $\forall x\ \neg\neg\varphi$ também é uma sentença. Assim , segue do Teorema da Dedução (Teorema 4.2.10)

$$\Sigma^* \vdash (\forall x\ \neg\neg\varphi \to \forall x\ \varphi).$$

Com (CP) obtemos

$$\Sigma^* \vdash (\neg\forall x\ \varphi \to \neg\forall x\ \neg\neg\varphi),$$

e por $\neg\forall x\ \varphi \in \Sigma^*$ finalmente $\exists x\ \neg\varphi \in \Sigma^*$. Pela propriedade (II) para pelo menos um $t \in TC$ vale

$$\Sigma^* \vdash (\exists x\ \neg\varphi \to \neg\varphi(x/t)).$$

Assim, concluímos que $\neg\varphi(x/t) \in \Sigma^*$ para algum $t \in TC$. Então pela propriedade (I) não pode valer $\varphi(x/t) \in \Sigma^*$.

■

4.4 Semântica da lógica de primeira ordem

Nesta seção falaremos da parte semântica de uma linguagem formal de primeira ordem $\mathcal{L}$, ou seja, da teoria do *significado* e da *validade*. Vamos aqui definir validade de uma $\mathcal{L}$-fórmula em um certo domínio (que será chamado de $\mathcal{L}$-estrutura), e vamos também estabelecer quando é que uma $\mathcal{L}$-estrutura pode ser considerada um "modelo" para um dado "sistema de axiomas".

Definição 4.4.1 *Fixada uma linguagem $\mathcal{L} = (\lambda, \mu, K)$, uma $\mathcal{L}$-estrutura $\mathfrak{A}$ fica determinada pelos seguintes dados:*

- um conjunto não vazio, chamado domínio de $\mathfrak{A}$, que denotaremos por $|\mathfrak{A}|$ ou, às vezes, simplesmente por A;

- uma relação $\lambda(i)$ ária sobre A, para cada $i \in I$, e que denotamos por $R_i^{\mathfrak{A}}$

- uma função $\mu(j)$-ária sobre A, para cada $j \in J$, e que denotamos por $f_j^{\mathfrak{A}}$;

- um elemento fixado de A, para cada $k \in K$, e que denotamos por $c_k^{\mathfrak{A}}$.

Resumimos todos estes dados escrevendo

$$\mathfrak{A} = \left\langle A; (R_i^{\mathfrak{A}})_{i\in I}; (f_j^{\mathfrak{A}})_{j\in J}; (c_k^{\mathfrak{A}})_{k\in K} \right\rangle .$$

Chamamos tais relações, funções e elementos, de interpretações das relações, funções e constantes da linguagem $\mathcal{L}$ na $\mathcal{L}$-estrutura $\mathfrak{A}$.

Exemplo 4.4.2 *Para as linguagens que enunciamos no Exemplo 4.1.4 temos, por exemplo, as seguintes estruturas:*

1) Uma estrutura para grupos abelianos totalmente ordenados:

Temos aqui os símbolos $<, +$ e 0 a serem interpretados. Dado um conjunto A não vazio, temos uma estrutura

$$\mathfrak{A} = \left\langle A; <^{\mathfrak{A}}; +^{\mathfrak{A}}; 0^{\mathfrak{A}} \right\rangle$$

para grupos abelianos totalmente ordenados. Omitiremos índices superiores quando for conveniente, escrevendo apenas

$$\mathfrak{A} = \langle A; <; +; 0 \rangle$$

2) Uma estrutura para anéis e corpos:

Aqui temos dois símbolos funcionais, $\cdot$ e $+$, e dois símbolos constantes, 0 e 1, a serem interpretados. Novamente, se A é não vazio, temos uma estrutura

$$\mathfrak{A} = \langle A; +^{\mathfrak{A}}, \cdot^{\mathfrak{A}}; 0^{\mathfrak{A}}, 1^{\mathfrak{A}} \rangle$$

ou, quando não houver ambigüidade,

$$\mathfrak{A} = \langle A; +, \cdot\ ; 0, 1 \rangle .$$

3) Uma estrutura para corpos valorizados:

Interpretamos aqui todos os símbolos da linguagem de corpos e um símbolo relacional adicional V, obtendo a estrutura:

$$\mathfrak{A} = \langle A; V^{\mathfrak{A}}; +^{\mathfrak{A}}, \cdot^{\mathfrak{A}}; 0^{\mathfrak{A}}, 1^{\mathfrak{A}} \rangle$$

ou simplesmente

$$\mathfrak{A} = \langle A; V; +, \cdot\ ; 0, 1 \rangle .$$

Salientamos também que, sendo $\mathcal{L}$ uma linguagem de primeira ordem, só podemos utilizar os quantificadores $\forall u$ e $\exists v$ sobre os domínios de $\mathcal{L}$-estruturas.

Definição 4.4.3 *Definimos uma avaliação de variáveis em $\mathfrak{A}$ como uma aplicação*

$$h : Vbl \longrightarrow |\mathfrak{A}| .$$

Dados uma avaliação em $\mathfrak{A}$ e $a \in |\mathfrak{A}|$, podemos definir outra avaliação

por:

$$h(x,a)(v) = \begin{cases} h(v), & \text{para } v \neq x \\ a, & \text{para } v = x \end{cases}$$

para cada $x \in Vbl$.

Note que as avaliações h e $h(x,a)$ coincidem em todas as variáveis diferentes de x. E, evidentemente,

$$h(x, h(x)) = h.$$

Definição 4.4.4 *O valor de um termo (interpretado) t pela avaliação h em $\mathfrak{A}$, denotado por $t^{\mathfrak{A}}[h]$, é definido por recursão sobre a construção de termos:*

$$\begin{aligned} v^{\mathfrak{A}}[h] &:= h(v) \\ c_k^{\mathfrak{A}}[h] &:= c_k^{\mathfrak{A}} \\ f_j(t_1, ..., t_{\mu(j)})^{\mathfrak{A}}[h] &:= f_j^{\mathfrak{A}}(t_1^{\mathfrak{A}}[h], ..., t_{\mu(j)}^{\mathfrak{A}}[h]). \end{aligned}$$

Note que de fato, com isto, além de determinarmos o valor dos termos mais simples, as variáveis e constantes, o valor de cada termo fica estipulado.

Para expressarmos a validade de uma fórmula (interpretada) φ por uma avaliação h em uma $\mathcal{L}$-estrutura $\mathfrak{A}$ fazemos uso do símbolo "$\models$", escrevendo

$$\mathfrak{A} \models \varphi[h]$$

(leia-se "em $\mathfrak{A}$ vale φ por h") ou

$$\mathfrak{A} \not\models \varphi[h]$$

para o caso contrário.

Definição 4.4.5 *Dadas uma $\mathcal{L}$-estutura $\mathfrak{A}$ e uma avaliação h de $\mathfrak{A}$, se*

$t_1, ..., t_{\lambda(i)} \in Tm_{\mathcal{L}}$ *e* $\varphi, \psi \in Fml_{\mathcal{L}}$, *temos:*

(1)	$\mathfrak{A} \models (t_1 \doteq t_2)[h]$	*se e só se*	$t_1^{\mathfrak{A}}[h] = t_2^{\mathfrak{A}}[h]$
(2)	$\mathfrak{A} \models R_i(t_1, ..., t_{\lambda(i)})[h]$	*se e só se*	$R_i^{\mathfrak{A}}(t_1^{\mathfrak{A}}[h], ..., t_{\lambda(i)}^{\mathfrak{A}}[h])$
(3)	$\mathfrak{A} \models \neg\varphi[h]$	*se e só se*	$\mathfrak{A} \not\models \varphi[h]$
(4)	$\mathfrak{A} \models (\varphi \wedge \psi)[h]$	*se e só se*	$(\mathfrak{A} \models \varphi[h]$ *e* $\mathfrak{A} \models \psi[h])$
(5)	$\mathfrak{A} \models \forall x\ \varphi[h]$	*se e só se*	$\mathfrak{A} \models \varphi[h(x, a)]$, *para todo* $a \in \lvert\mathfrak{A}\rvert$

Observamos que, no último caso, temos uma variável x limitada pelo quantificador $\forall x$, e pela definição dada, a fórmula à esquerda vale se pudermos verificar a validade de todas as fórmulas $\varphi[h(x, a)]$ obtidas pela substituição de x por qualquer elemento do domínio da estrutura na fórmula $\varphi[h]$. (Salientamos que neste caso e nos outros acima a definição de validade coincide realmente com nossa intuição.)

Obtemos imediatamente, da definição acima e das definições de $\wedge, \rightarrow, \leftrightarrow$ e $\exists$:

(6)	$\mathfrak{A} \models (\varphi \vee \psi)[h]$	se e só se	$(\mathfrak{A} \models \varphi[h]$	ou	$\mathfrak{A} \models \psi[h])$
(7)	$\mathfrak{A} \models (\varphi \rightarrow \psi)[h]$	se e só se	$(\mathfrak{A} \models \varphi[h]$	implica	$\mathfrak{A} \models \psi[h])$
(8)	$\mathfrak{A} \models (\varphi \leftrightarrow \psi)[h]$	se e só se	$(\mathfrak{A} \models \varphi[h]$	se e só se	$\mathfrak{A} \models \psi[h])$
(9)	$\mathfrak{A} \models \exists x\ \varphi[h]$	se e só se	existe $a \in \lvert\mathfrak{A}\rvert$	tal que	$\mathfrak{A} \models \varphi[h(x, a)]$

Aqui os termos "ou", "implica", "se e só se" e "existe um a" , são utilizados com o sentido matemático usual, que, por sua vez, coincide com o sentido dado pela Lógica, ou seja, o "ou" não é exclusivo, e uma afirmação implica outra, caso a hipótese seja falsa, ou caso a hipótese seja verdadeira e a conclusão também verdadeira.

Apresentamos agora um exemplo para motivar o próximo resultado.

Exemplo 4.4.6 *Considere, na linguagem dos grupos abelianos totalmente ordenados, a estrutura* $\mathfrak{A} = \langle \mathbb{Z};\ <^{\mathfrak{A}};\ +^{\mathfrak{A}};\ 0^{\mathfrak{A}} \rangle$ *dos números inteiros. Aplicamos a definição de validade por uma avaliação* h *sobre a fórmula*

$$\exists v_0\ (0 < v_0 \wedge v_0 < v_1).$$

e obtemos :

$$\mathfrak{A} \models \exists v_0\ (0 < v_0 \wedge v_0 < v_1)[h] \quad \textit{se e só se} \quad \textit{existe um } a \in \mathbb{Z} \textit{ tal que } \mathfrak{A} \models (0 < v_0 \wedge v_0 < v_1)[h(v_0, a)]$$

$$\textit{se e só se} \quad \textit{existe um } a \in \mathbb{Z} \textit{ tal que } (0^{\mathfrak{A}} <^{\mathfrak{A}} a \quad e \quad a <^{\mathfrak{A}} h(v_1)).$$

Este exemplo mostra que a definição de validade se comporta como gostaríamos e, mais ainda, nos indica que, para a relação $\models$, precisamos apenas do efeito de h sobre as variáveis livres de uma fórmula φ para determinar se ela é válida ou não. Mais precisamente:

Lema 4.4.7 *Sejam h e h' avaliações na $\mathcal{L}$-estrutura $\mathfrak{A}$. Então vale:*

(a) h e h' coincidem nas variáveis que aparecem no $\mathcal{L}$-termo t, então $t^{\mathfrak{A}}[h] = t^{\mathfrak{A}}[h']$

(b) h e h' coincidem nas variáveis livres da $\mathcal{L}$-fórmula φ, então vale:

$$\mathfrak{A} \models \varphi[h] \quad \textit{se e só se} \quad \mathfrak{A} \models \varphi[h'].$$

Prova. *(a)* A prova é por indução sobre a construção dos termos a partir das seguintes observações:

$$v^{\mathfrak{A}}[h'] = h'(v) = h(v) = v^{\mathfrak{A}}[h]$$

$$c_k^{\mathfrak{A}}[h'] = c_k^{\mathfrak{A}} = c_k^{\mathfrak{A}}[h]$$

$$\begin{aligned} f_j(t_1, ..., t_{\mu(j)})^{\mathfrak{A}}[h'] &= f_j^{\mathfrak{A}}(t_1^{\mathfrak{A}}[h'], ..., t_{\mu(j)}^{\mathfrak{A}}[h']) \\ &= f_j^{\mathfrak{A}}(t_1^{\mathfrak{A}}[h], ..., t_{\mu(j)}^{\mathfrak{A}}[h]) = f_j(t_1, ..., t_{\mu(j)})^{\mathfrak{A}}[h]. \end{aligned}$$

(*b*) A prova é por indução sobre a construção das fórmulas, utilizando também o item (*a*).

$$\begin{aligned}
\mathfrak{A} \models (t_1 \doteq t_2)[h'] &\Leftrightarrow t_1^{\mathfrak{A}}[h'] = t_2^{\mathfrak{A}}[h'] \\
&\overset{(a)}{\Leftrightarrow} t_1^{\mathfrak{A}}[h] = t_2^{\mathfrak{A}}[h] \\
&\Leftrightarrow \mathfrak{A} \models (t_1 \doteq t_2)[h].
\end{aligned}$$

$$\begin{aligned}
\mathfrak{A} \models R_i(t_1, ...)[h'] &\Leftrightarrow R_i^{\mathfrak{A}}(t_1^{\mathfrak{A}}[h'], ...) \\
&\overset{(a)}{\Leftrightarrow} R_i^{\mathfrak{A}}(t_1^{\mathfrak{A}}[h], ...) \\
&\Leftrightarrow \mathfrak{A} \models R_1(t_1, ...)[h].
\end{aligned}$$

$$\begin{aligned}
\mathfrak{A} \models \neg\varphi[h'] &\Leftrightarrow \mathfrak{A} \not\models \varphi[h'] \\
&\overset{\textit{Hip. Ind.}}{\Leftrightarrow} \mathfrak{A} \not\models \varphi[h] \\
&\Leftrightarrow \mathfrak{A} \models \neg\varphi[h].
\end{aligned}$$

$$\begin{aligned}
\mathfrak{A} \models (\varphi \wedge \psi)[h'] &\Leftrightarrow (\mathfrak{A} \models \varphi[h'] \text{ e } \mathfrak{A} \models \psi[h']) \\
&\overset{\textit{Hip. Ind.}}{\Leftrightarrow} (\mathfrak{A} \models \varphi[h] \text{ e } \mathfrak{A} \models \psi[h]) \\
&\Leftrightarrow \mathfrak{A} \models (\varphi \wedge \psi)[h].
\end{aligned}$$

$$\begin{aligned}
\mathfrak{A} \models \forall x\ \varphi[h'] &\Leftrightarrow \mathfrak{A} \models \varphi[h'(x, a)] \quad \text{para todo} \quad a \in A \\
&\overset{\textit{Hip. Ind.}}{\Leftrightarrow} \mathfrak{A} \models \varphi[h(x, a)] \quad \text{para todo} \quad a \in A \\
&\Leftrightarrow \mathfrak{A} \models \forall x\ \varphi[h].
\end{aligned}$$

Observe que, por hipótese, as avaliações $h'(x, a)$ e $h(x, a)$ alteram igualmente as variáveis livres de φ.

■

Em particular observamos que, pelo lema acima, a validade de uma sentença α (fórmula que não possui variáveis livres) por h em $\mathfrak{A}$ não depende da avaliação h em $\mathfrak{A}$ considerada. Isto quer dizer que

$$\mathfrak{A} \models \alpha[h] \quad \text{se e só se} \quad \mathfrak{A} \models \alpha[h']$$

para toda $\alpha \in Sent_{\mathcal{L}}$ e todas as avaliações h e h' em $\mathfrak{A}$.

Definimos a seguir validade universal de uma fórmula φ em uma $\mathcal{L}$-estrutura $\mathfrak{A}$.

Definição 4.4.8 *Dizemos que uma $\mathcal{L}$-fórmula φ vale universalmente em $\mathfrak{A}$, e escrevemos*

$$\mathfrak{A} \models \varphi,$$

quando, para toda avaliação h nesta, vale

$$\mathfrak{A} \models \varphi[h].$$

Salientamos a seguinte equivalência:

$$\mathfrak{A} \models \varphi \quad \text{se e só se} \quad \mathfrak{A} \models \forall\varphi, \tag{77}$$

onde $\forall\varphi$ está no lugar de $\forall x_1, ..., x_n\ \varphi$, com $Fr(\varphi) \subset \{x_1, ..., x_n\}$ (veja Notação 4.1.12). De fato, vale

$$\mathfrak{A} \models \varphi \quad \text{se e só se} \quad \mathfrak{A} \models \forall x\ \varphi,$$

pois

$$\begin{aligned}
&\mathfrak{A} \models \varphi \text{ se e só se } \mathfrak{A} \models \varphi[h] \text{ para toda a valiacão } h \\
\text{se e só se } &\mathfrak{A} \models \varphi[h(x,a)] \text{ para toda } h \text{ e todo } a \in |\mathfrak{A}| \\
\text{se e só se } &\mathfrak{A} \models \forall x\ \varphi[h] \text{ para toda } h \\
\text{se e só se } &\mathfrak{A} \models \forall x\ \varphi
\end{aligned}$$

Daí, para obter-se (77), basta fazermos uso da equivalência acima n vezes.

Uma vez estabelecido o conceito de validade, estamos em condições de definir o que é afinal um modelo e responder a questão da seção anterior, ou seja: o que deve ocorrer para que se tenha $\Sigma \nvdash \varphi$.

Definição 4.4.9 *Dado um conjunto $\Sigma \subset Sent_{\mathcal{L}}$, um modelo de Σ é uma*

$\mathcal{L}$-estrutura $\mathfrak{A}$ na qual valem todas as sentenças de Σ, ou seja,

$$\mathfrak{A} \models \sigma, \text{ para toda } \sigma \in \Sigma.$$

Também escreveremos

$$\mathfrak{A} \models \Sigma$$

para representar este fato.

Teorema 4.4.10 (Teorema da Completude de Gödel) *Sejam*

$$\Sigma \subset Sent_{\mathcal{L}} \quad e \quad \varphi \in Sent_{\mathcal{L}}.$$

Se

$$\Sigma \nvdash \varphi$$

então existe um "contra-exemplo", ou seja, existe uma $\mathcal{L}$-estrutura $\mathfrak{A}$ que é um modelo de Σ, no qual não vale φ, o que pela Definição 4.4.5, é equivalente a $\mathfrak{A}$ ser um modelo de $\Sigma \cup \{\neg\varphi\}$.

Prova. Se Σ é contraditório então o resultado vale por vacuidade, pela Observação 4.3.2.

Suponhamos então que Σ é não-contraditório. Como

$$\Sigma \nvdash \varphi,$$

temos, pelo Lema 4.3.3, o conjunto $\Sigma_1 = \Sigma \cup \{\neg\varphi\}$ é não-contraditório. Assim, basta mostrar que cada conjunto $\Sigma \subset Sent_{\mathcal{L}}$ não-contraditório possui um modelo.

Empregamos sobre tal conjunto o Teorema 4.3.5 e o Teorema 4.3.6, obtendo uma sobre-linguagem $\mathcal{L}'$ de $\mathcal{L} = (I, J, K)$ e um conjunto maximal não contraditório $\Sigma^* \subset Sent_{\mathcal{L}'}$ com as propriedades (I) e (II) (veja (69).

Seja

$$A = TC/\approx$$

o conjunto das classes de equivalência dos termos constantes da linguagem $\mathcal{L}'$ construído na seção anterior. Sejam $\mathfrak{R}_i$ (para $i \in I$) , $\mathfrak{f}_j$ (para $j \in J$) e

$\overline{c_k}$ (para $k \in K'$), definidos como as interpretações dos símbolos relacionais R_i, funcionais f_j e constantes c_k, respectivamente, no conjunto A (veja (74),(75) e (76)):

$$\mathfrak{R}_i = R_i^{\mathfrak{A}} \ , \ \mathfrak{f}_j = f_j^{\mathfrak{A}} \ , \ \overline{c_k} = c_k^{\mathfrak{A}}.$$

Assim,

$$\mathfrak{A} = \langle A; (\mathfrak{R}_i)_{i\in I}; (\mathfrak{f}_j)_{j\in J}; (\overline{c_k})_{k\in K'} \rangle \ ,$$

é uma $\mathcal{L}'$-estrutura. Queremos mostrar que $\mathfrak{A}$ é um modelo para Σ^*.

Afirmamos inicialmente que, para cada avaliação h de $\mathfrak{A}$, para todo $t \in TC$

$$t^{\mathfrak{A}}[h] = \overline{t}. \tag{78}$$

A prova é por indução sobre a construção de um termo constante. A base de indução é clara, pois neste caso temos obviamente $c_k^{\mathfrak{A}} = \overline{c_k}$, para todo $k \in K'$. Para o passo de indução temos:

$$\begin{array}{lll} f_j(t_1, ..., t_{\mu(j)})^{\mathfrak{A}}[h] & = & f_j^{\mathfrak{A}}(t_1^{\mathfrak{A}}[h], ..., t_{\mu(j)}^{\mathfrak{A}}[h]) \\ & \overset{\text{hip.indução}}{=} & \mathfrak{f}_j(\overline{t_1}, ..., \overline{t_{\mu(j)}}) \\ & \overset{(75)}{=} & \overline{f_j(t_1, ..., t_{\mu(j)})}. \end{array}$$

Afirmamos também que, para cada $\varphi \in Sent_{\mathcal{L}'}$ e cada avaliação h em $\mathfrak{A}$, vale

$$\mathfrak{A} \models \varphi[h] \quad \text{se e só se} \quad \varphi \in \Sigma^* \tag{79}$$

o que nos mostra, em particular, que $\mathfrak{A}$ é um modelo para Σ^*. Esta equivalência é também provada por indução sobre a construção de φ, mais precisamente, sobre o número de símbolos lógicos $\neg$, $\wedge$ e $\forall$ utilizados na construção de φ.

Se este número que número é 0, então temos que φ é uma fórmula atômica, ou seja, é da forma $t_1 \doteq t_2$ ou da forma $R_i(t_1, ..., t_{\lambda(i)})$.

No primeiro caso temos

$$\begin{array}{lll} \mathfrak{A} \models (t_1 \doteq t_2)[h] & \overset{\text{Def.4.4.5(1)}}{\Leftrightarrow} & t_1^{\mathfrak{A}}[h] = t_2^{\mathfrak{A}}[h] \\ & \overset{(78)}{\Leftrightarrow} & \overline{t_1} = \overline{t_2} \\ & \overset{(74)}{\Leftrightarrow} & \Sigma^* \vdash (t_1 \doteq t_2) \\ & \overset{\text{Lema4.3.8}}{\Leftrightarrow} & (t_1 \doteq t_2) \in \Sigma^* \end{array}$$

e, no segundo caso,

$$\begin{array}{lll} \mathfrak{A} \models R_i(t_1, ..., t_{\lambda(i)})[h] & \overset{\text{Def.4.4.5(2)}}{\Leftrightarrow} & R_i^{\mathfrak{A}}(t_1^{\mathfrak{A}}[h], ..., t_{\lambda(i)}^{\mathfrak{A}}[h]) \\ & \overset{(78)}{\Leftrightarrow} & \mathfrak{R}_i(\overline{t_1}, ..., \overline{t_{\lambda(i)}}) \\ & \overset{(74)}{\Leftrightarrow} & \Sigma^* \vdash R_i(t_1, ..., t_{\lambda(i)}) \\ & \overset{\text{Lema 4.3.8}}{\Leftrightarrow} & R_i(t_1, ..., t_{\lambda(i)}) \in \Sigma^*. \end{array}$$

Suponhamos agora que φ é da forma $\neg\alpha$, onde α é uma sentença; então

$$\begin{array}{lll} \mathfrak{A} \models \neg\alpha[h] & \overset{\text{Def.4.4.5(3)}}{\Leftrightarrow} & \mathfrak{A} \not\models \alpha[h] \\ & \overset{\text{hip.ind.}}{\Leftrightarrow} & \alpha \notin \Sigma^* \\ & \overset{\text{Teorema 4.3.9(a)}}{\Leftrightarrow} & \neg\alpha \in \Sigma^*. \end{array}$$

E, se φ é da forma $(\alpha \wedge \beta)$, onde α e β são também sentenças; então

$$\begin{array}{lll} \mathfrak{A} \models (\alpha \wedge \beta)[h] & \overset{\text{Def.4.4.5(4)}}{\Leftrightarrow} & (\mathfrak{A} \models \alpha[h] \quad \text{e} \quad \mathfrak{A} \models \beta[h]) \\ & \overset{\text{hip.ind.}}{\Leftrightarrow} & (\alpha \in \Sigma^* \quad \text{e} \quad \beta \in \Sigma^*) \\ & \overset{\text{Teorema 4.3.9(b)}}{\Leftrightarrow} & (\alpha \wedge \beta) \in \Sigma^*. \end{array}$$

Resta-nos mostrar (79) no caso em que φ é da forma $\forall x\ \psi$. Para tal, vamos precisar do seguinte resultado a ser provado logo depois

Lema 4.4.11 *Sejam φ uma $\mathcal{L}$-fórmula e t um $\mathcal{L}$-termo livre de x em φ. Então, para toda avaliação h em uma $\mathcal{L}$-estrutura $\mathfrak{A}$ com $a = t^{\mathfrak{A}}[h]$:*

$$\mathfrak{A} \models \varphi[h(x, a)] \quad \textit{se e só se} \quad \mathfrak{A} \models \varphi(x/t)[h]$$

Completando então a prova do Teorema de Gödel: se a sentença φ é da forma $\forall x\ \psi$, então $Fr(\psi) \subset \{x\}$; daí, para todo $t \in TC$, evidentemente $\psi(x/t)$ é novamente uma sentença, envolvendo em sua construção um número menor de símbolos lógicos do que $\forall x\ \psi$.

Obtemos, por indução:

$$\begin{array}{lll}
\mathfrak{A} \models \forall x\ \psi[h] & \overset{\text{Def.4.4.5(5)}}{\Leftrightarrow} & \mathfrak{A} \models \psi[h(x,a)] \quad \text{para todo} \quad a \in A = TC/\approx \\
& \Leftrightarrow & \mathfrak{A} \models \psi[h(x,\bar{t})] \quad \text{para todo} \quad t \in TC. \\
& \overset{\text{Lema 4.4.11}}{\underset{(78)}{\Leftrightarrow}} & \mathfrak{A} \models \psi(x/t)[h] \quad \text{para todo} \quad t \in TC \\
& \overset{\text{hip.ind.}}{\Leftrightarrow} & \psi(x/t) \in \Sigma^* \quad \text{para todo} \quad t \in TC \\
& \overset{\text{Teorema 4.3.9(c)}}{\Leftrightarrow} & \forall x\ \psi \in \Sigma^*
\end{array}$$

Obtemos assim que, nesta $\mathcal{L}'$-estrutura $\mathfrak{A}$ vale $\varphi \in \Sigma^*$, para toda $\mathcal{L}'$-sentença φ que satisfaz $\mathfrak{A} \models \varphi[h]$, para toda avaliação h. Com isto é claro que na $\mathcal{L}$-estrutura

$$\langle A; (\mathfrak{R})_{i\in I}; (\mathfrak{f}_j)_{j\in J}; (\overline{c_k})_{k\in K}\rangle$$

vale toda $\mathcal{L}$-sentença $\varphi \in \Sigma$. Assim Σ possui um modelo.

■

Da demonstração acima obtemos:

Corolário 4.4.12 *Todo Σ não-contraditório admite um modelo.*

Prova.[Prova do Lema 4.4.11] Inicialmente observamos que, para todo termo t_1, é possível mostrar por indução sobre sua construção que, como $a = t^{\mathfrak{A}}[h]$,

$$t_1^{\mathfrak{A}}[h(x,a)] = t_1(x/t)^{\mathfrak{A}}[h]. \tag{80}$$

Agora provamos a equivalência afirmada para a fórmula φ através de indução sobre a sua construção.

- Se φ for uma fórmula atômica do tipo $t_1 \doteq t_2$ então

$$\begin{array}{lll}
\mathfrak{A} \models (t_1 \doteq t_2)[h(x,a)] & \Leftrightarrow & t_1^{\mathfrak{A}}[h(x,a)] = t_2^{\mathfrak{A}}[h(x,a)] \\
& \overset{(80)}{\Leftrightarrow} & t_1(x/t)^{\mathfrak{A}}[h] = t_2(x/t)^{\mathfrak{A}}[h] \\
& \Leftrightarrow & \mathfrak{A} \models (t_1 \doteq t_2)(x/t)[h],
\end{array}$$

onde $(t_1 \doteq t_2)(x/t)[h]$ é idêntica a $t_1(x/t) \doteq t_2(x/t)$.

- A outra fórmula atômica é tratada de maneira análoga.

- Os casos em que φ é da forma $\neg\alpha$ ou $(\alpha \wedge \beta)$ seguem da validade para α e β desta forma de escrita.

- Falta-nos abordar o caso em que φ é da forma $\forall y\ \psi$. Aqui distinguimos dois casos.

Caso 1 : Se $x = y$ ou $x \notin Fr(\psi)$.

Sob esta hipótese vale que $x \notin Fr(\forall y\ \psi)$. Disto e do Lema 4.4.7$(b)$ temos

$$\mathfrak{A} \models \forall y\ \psi[h(x,a)] \Leftrightarrow \mathfrak{A} \models \forall y\ \psi[h]$$

Esta porém é a afirmação, pois neste caso $(\forall y\ \psi)(x/t) = \forall y\ \psi$ (veja Definição 4.1.9).

Caso 2 : Se $x \neq y$ e $x \in Fr(\psi)$.

Como, por hipótese, t é livre de x em $\forall y\ \psi$, neste caso y não pode aparecer em t, pois caso contrário, ao substituir x por t teríamos que a variável y cairia no alcance de $\forall y$ (veja Definição 4.1.10). Com o Lema 4.4.7 segue que, para cada $a' \in |\mathfrak{A}|$,

$$a = t^{\mathfrak{A}}[h] = t^{\mathfrak{A}}[h(y,a')]$$

Definindo $h' = h(y,a')$, temos, considerando a avaliação $h(x,a)$: $a = t^{\mathfrak{A}}[h']$ e

$$\begin{aligned}
\mathfrak{A} \models \forall y\ \psi[h(x,a)] \quad &\Leftrightarrow \quad \mathfrak{A} \models \psi[h(x,a)(y,a')] \quad \text{para todo} \quad a' \in |\mathfrak{A}| \\
&\overset{\text{Lema 4.4.7}}{\Leftrightarrow} \quad \mathfrak{A} \models \psi[h'(x,a)] \quad \text{para todo} \quad a' \in |\mathfrak{A}| \\
&\Leftrightarrow \quad \mathfrak{A} \models \psi[h'(x,t^{\mathfrak{A}}[h'])] \quad \text{para todo} \quad a' \in |\mathfrak{A}| \\
&\overset{\text{Hip.Ind.}}{\Leftrightarrow} \quad \mathfrak{A} \models \psi(x/t)[h'] \quad \text{para todo} \quad a' \in |\mathfrak{A}| \\
&\Leftrightarrow \quad \mathfrak{A} \models \psi(x/t)[h(y,a')] \quad \text{para todo} \quad a' \in |\mathfrak{A}| \\
&\Leftrightarrow \quad \mathfrak{A} \models \forall y\ \psi(x/t)[h].
\end{aligned}$$

■

O próximo teorema nos garante a coerência do conceito de prova: ele nos diz que toda sentença que pode ser deduzida de um conjunto de sentenças Σ também é válida em todo modelo de Σ.

Teorema 4.4.13 *Sejam $\Sigma \subset Sent_{\mathcal{L}}$ e $\varphi \in Sent_{\mathcal{L}}$ com $\Sigma \vdash \varphi$. Então φ vale em cada modelo de Σ.*

Prova. Sejam $\mathfrak{A}$ um modelo de Σ e $(\varphi_1, ..., \varphi_n)$ uma prova de φ a partir de Σ. Mostraremos que $\mathfrak{A} \models \varphi$ por indução sobre n . Com isto, em particular, fica provado o teorema.

Para $n = 1$ temos que $\varphi_1 \in \Sigma$ ou é um axioma lógico.

- No primeiro caso, temos automaticamente que φ_1 vale em $\mathfrak{A}$.

- Se φ_1 é uma tautologia obtida, digamos, de uma tautologia lógica Φ com variáveis predicativas $A_0, ..., A_m$ pela substituição de A_i por uma $\mathcal{L}$-fórmula ψ_i para $0 \leq i \leq m$ (veja Definição 4.2.4) então, para toda avaliação lógica B, temos que $B(\Phi) = V$ (veja Definição 4.2.3).

Dada uma avaliação h da linguagem $\mathcal{L}$, definimos a avaliação lógica B_h por

$$B_h(A) = V \quad \text{sse} \quad \mathfrak{A} \models \psi[h],$$

para cada forma predicativa A, onde ψ é a $\mathcal{L}$-fórmula que corresponde a A. Como Φ é uma tautologia, temos que, em particular,

$$B_h(\Phi) = V,$$

para toda avaliação h, e portanto,

$$\mathfrak{A} \models \varphi_1[h],$$

para toda avaliação h. Assim temos, pela Definição 4.4.8, que

$$\mathfrak{A} \models \varphi_1.$$

- O caso de φ_1 ser um axioma de identidade lógica segue de maneira análoga.

- Resta-nos o caso em que φ_1 é um axioma de quantificador:

- Se φ_1 é da forma (A_2) (veja Axioma 4.2.5), digamos,

$$\forall x\ (\alpha \to \beta) \to (\alpha \to \forall x\ \beta),$$

onde $x \notin Fr(\alpha)$, pelo emprego da definição de validade falta provar que para cada h, a hipótese

$$\mathfrak{A} \models (\alpha \to \beta)[h(x,a)] \quad \text{para todo} \quad a \in |\mathfrak{A}|$$

implica:

$$\text{caso } \mathfrak{A} \models \alpha[h] \text{ então } \mathfrak{A} \models \beta[h(x,a)] \text{ para todo } a \in |\mathfrak{A}|.$$

Seja então $a \in |\mathfrak{A}|$ e suponhamos que $\mathfrak{A} \models \alpha[h]$. Como $x \notin Fr(\alpha)$ temos, pelo Lema 4.4.7 primeiramente

$$\mathfrak{A} \models \alpha[h(x,a)],$$

para todo $a \in |\mathfrak{A}|$. Pela hipótese, obtemos portanto

$$\mathfrak{A} \models \beta[h(x,a)],$$

para todo $a \in |\mathfrak{A}|$, o que queríamos provar.

- Se φ_1 é da forma $(A1)$ (veja Axioma 4.2.5), digamos,

$$\forall x\ \alpha \to \alpha(x/t),$$

sendo t livre de x em α, então, para cada avaliação h queremos provar que a hipótese

$$\mathfrak{A} \models \alpha[h(x,a)] \quad \text{para todo} \quad a \in A$$

implica

$$\mathfrak{A} \models \alpha(x/t)[h],$$

que, por sua vez, pelo Lema 4.4.11, é equivalente a

$$\mathfrak{A} \models \alpha[h(x, a)],$$

com $a = t^{\mathfrak{A}}[h]$. Mas isto, no entanto, é um caso especial da hipótese. Com isto encerramos a demonstração do caso $n = 1$.

Suponhamos agora que, para todo $i < n$, já tenhamos provado que

$$\mathfrak{A} \models \varphi_i.$$

Queremos então provar que

$$\mathfrak{A} \models \varphi_n.$$

- Se φ_n é um axioma lógico ou está em Σ, então obtemos $\mathfrak{A} \models \varphi_n$ pela base de indução.

- Se φ_n foi obtida por (MP), então existem $i, j < n$ tais que φ_j é da forma

$$(\varphi_i \to \varphi_n).$$

Para cada avaliação h temos portanto

$$\mathfrak{A} \models (\varphi_i \to \varphi_n)[h] \quad \text{e} \quad \mathfrak{A} \models \varphi_i[h].$$

Disto segue naturalmente que

$$\mathfrak{A} \models \varphi_n[h].$$

- Finalmente, se φ_n é obtida pela aplicação da regra lógica ($\forall$), então existem $i < n$ e uma variável x tais que φ_n é da forma

$$\forall x\, \varphi_i.$$

Mas vimos, logo após a Definição 4.4.8, que

$$\mathfrak{A} \models \varphi_i$$

é equivalente a

$$\mathfrak{A} \models \forall \varphi_i,$$

ou seja,

$$\mathfrak{A} \models \varphi_n.$$

■

Complementamos o Corolário 4.4.12 provando sua recíproca:

Corolário 4.4.14 *Um conjunto $\Sigma \subset Sent_{\mathcal{L}}$ é não-contraditório se e só se ele possui um modelo.*

Prova. Se Σ é não-contraditório, então, pelo Corolário 4.4.12, Σ possui um modelo . Reciprocamente, se Σ possui um modelo, então pelo Teorema 4.4.13 não podemos deduzir nehuma contradição de Σ. De fato, se tal fosse possível, pela Definição 4.3.1 teríamos $\Sigma \vdash (\neg\alpha \wedge \alpha)$, mas então o Teorema 4.4.13 implicaria a validade da sentença $(\neg\alpha \wedge \alpha)$ no tal modelo, o que é uma contradição, pois ela sempre toma o valor F (falso) por uma avaliação lógica.

■

O corolário acima reúne os importantes Teoremas 4.4.10 e 4.4.13. Ele é um dos mais fundamentais teoremas da Teoria dos Modelos.

Encerramos esta seção enunciando um resultado que pode ser provado com o Teorema de Gödel:

Teorema 4.4.15 *Um conjunto $\Sigma \subset Sent_{\mathcal{L}}$ possui um modelo se todo subconjunto finito Π de Σ possui um modelo.*

Prova. Suponha que Σ não possui nenhum modelo. Então, pelo Corolário 4.4.14, Σ é contraditório. Portanto pela Observação 4.3.2 conseguimos, a partir de Σ, provar uma contradição. Em tal prova fazemos uso de apenas um número finito de elementos de Σ, pois toda prova tem um número finito de passos. Então existe um subconjunto finito Π de Σ que é contraditório. Novamente, pelo Corolário 4.4.14, Π não possui nenhum modelo.

■

Observe que a prova do teorema acima depende do fato crucial de nossas provas terem um número finito de passos. Vemos também que ele foi provado com uso do Teorema da Completude de Gödel, sendo este último de caráter puramente lógico. No entanto é possível dar uma prova usando somente conceitos da Teoria dos Modelos, mais precisamente, usando os conceitos de "linguagem formal", "modelo" e "Ultraprodutos". Faremos isto na seção 4.11. No entanto, o apresentamos aqui porque também utilizaremos este resultado na Seção 4.9 (veja Corolário 4.9.11) e na Seção 4.10 (veja Lema 4.10.5).

4.5 Axiomatizando uma Teoria Matemática

Introduzimos nesta seção os conceitos de classe de modelos e de teoria que serão importantes para o estudo que segue.

Definição 4.5.1 *Sejam $\mathcal{L} = (\lambda, \mu, K)$ uma linguagem formal e seja M uma classe não vazia de $\mathcal{L}$-estruturas. A $\mathcal{L}$-teoria de M é o conjunto*

$$Th_{\mathcal{L}}(M) := \{\alpha \in Sent_{\mathcal{L}} \mid \mathfrak{A} \models \alpha \text{ para toda } \mathfrak{A} \in M\}.$$

Quando estiver claro em qual linguagem trabalhamos usaremos apenas $Th(M)$, e se M é um conjunto unitário (por exemplo, $M = \{\mathfrak{A}\}$), então denotamos $Th_{\mathcal{L}}(\{\mathfrak{A}\})$ simplesmente por $Th_{\mathcal{L}}(\mathfrak{A})$ ou $Th(\mathfrak{A})$. Assim,

$$Th_{\mathcal{L}}(\mathfrak{A}) = \{\alpha \in Sent_{\mathcal{L}} \mid \mathfrak{A} \models \alpha\}.$$

Observamos que $Th_{\mathcal{L}}(M)$ é sempre não vazio pois sempre vale

$$\mathfrak{A} \models (x \doteq x)$$

para qualquer $\mathcal{L}$-estrutura $\mathfrak{A}$.

Evidentemente, cada $\mathfrak{A} \in M$ é um modelo de $Th_{\mathcal{L}}(M)$.

O conjunto $Th_{\mathcal{L}}(M)$ possui duas propriedades importantes:

$$\begin{array}{l} \text{(A) } Th_{\mathcal{L}}(M) \text{ é não-contraditório.} \\ \text{(B) } Th_{\mathcal{L}}(M) \text{ é dedutivamente fechado.} \end{array} \tag{81}$$

A propriedade (A) segue do Corolário 4.4.14.

Mostremos então a propriedade (B). Suponhamos que $\alpha \in Sent_{\mathcal{L}}$ e que $Th_{\mathcal{L}}(M) \vdash \alpha$. Como cada $\mathfrak{A} \in M$ é um modelo de $Th_{\mathcal{L}}(M)$, temos, pelo Teorema 4.4.13, que cada $\mathfrak{A} \in M$ é , em particular, um modelo de $\{\alpha\}$. Assim, pela definição de $Th_{\mathcal{L}}(M)$,

$$\alpha \in Th_{\mathcal{L}}(M),$$

e portanto, pela Definição 4.3.7, $Th_{\mathcal{L}}(M)$ é dedutivamente fechado.

A seguir, generalizamos a definição acima:

Definição 4.5.2 *Dizemos que um conjunto $T \subset Sent_{\mathcal{L}}$ é uma $\mathcal{L}$-teoria, caso T satisfaça:*

- *T é não contraditório.*
- *T é dedutivamente fechado.*

Uma classe de $\mathcal{L}$-sentenças T, em particular uma $\mathcal{L}$-teoria, determina uma classe de $\mathcal{L}$-estruturas, chamada a classe dos modelos de T :

$$Mod_{\mathcal{L}}(T) = \{\mathfrak{A} \mid \mathfrak{A} \text{ é uma } \mathcal{L}\text{-estrutura e } \mathfrak{A} \models T\}.$$

Como consequência do Teorema da Completude de Gödel (Teorema 4.4.10), temos:

Corolário 4.5.3 *Dada uma $\mathcal{L}$-teoria $T \subset Sent_{\mathcal{L}}$, tem-se*

$$T = Th_{\mathcal{L}}(Mod_{\mathcal{L}}(T)).$$

Prova. Da Definição 4.5.1, segue que $T \subset Th_{\mathcal{L}}(Mod_{\mathcal{L}}(T))$, pois se $\alpha \in T$ obviamente α vale em todos os modelos de T, e portanto $\alpha \in Th_{\mathcal{L}}(Mod_{\mathcal{L}}(T))$.

Reciprocamente, se $\alpha \in Th_{\mathcal{L}}(Mod_{\mathcal{L}}(T))$ então

$$\mathfrak{A} \models \alpha$$

para toda $\mathcal{L}$-estrutura $\mathfrak{A}$ para a qual $\mathfrak{A} \models T$ (veja Definição 4.4.9). Ou seja, α vale em todos os modelos de T. Portanto, pelo Teorema da Completude de Gödel (Teorema 4.4.10), segue que

$$T \vdash \alpha.$$

Por ser T dedutivamente fechado, temos então

$$\alpha \in T,$$

e com isto concluímos:

$$T = Th_{\mathcal{L}}(Mod_{\mathcal{L}}(T)).$$

■

Observação 4.5.4 *Salientamos que não vale necessariamente*

$$Mod_{\mathcal{L}}(Th_{\mathcal{L}}(M)) = M,$$

onde M é uma classe qualquer de estruturas. De fato, se M for unitário, digamos, $M = \{\mathfrak{A}\}$, então teremos em $Mod_{\mathcal{L}}(Th_{\mathcal{L}}(M))$ todas as $\mathcal{L}$-estruturas elementarmente equivalentes a $\mathfrak{A}$, conceito que será introduzido na próxima seção. Mas se $|\mathfrak{A}|$ for infinito, temos mais do que uma destas estruturas, como também veremos na seção seguinte.

Definição 4.5.5 *Dado um conjunto de sentenças $\Sigma \subset Sent_{\mathcal{L}}$, denotamos por $Ded_{\mathcal{L}}(\Sigma)$ o conjunto das $\mathcal{L}$-sentenças que podem ser deduzidas (provadas) a partir de Σ. Ou seja:*

$$Ded_{\mathcal{L}}(\Sigma) = \{\alpha \in Sent_{\mathcal{L}} \mid \Sigma \vdash \alpha\}$$

Note que se $\{\alpha_1, ..., \alpha_n\} \vdash \alpha$ com $\alpha_1, ..., \alpha_n \in Ded_{\mathcal{L}}(\Sigma)$ então, por definição, conseguimos também uma prova de α a partir de Σ , e portanto $\alpha \in Ded_{\mathcal{L}}(\Sigma)$. Assim, $Ded_{\mathcal{L}}(\Sigma)$ é dedutivamente fechado e portanto tem chances de se tornar uma teoria: basta que seja também um conjunto não contraditório. Isto nos leva à seguinte

Definição 4.5.6 *Um sistema de axiomas para uma $\mathcal{L}$-teoria T é um conjunto $\Sigma \subset Sent_{\mathcal{L}}$ que satisfaz*

$$T = Ded_{\mathcal{L}}(\Sigma).$$

Pelo Teorema 4.4.13 vemos que se Σ é um sistema de axiomas para uma teoria T e $\alpha \in Ded_{\mathcal{L}}(\Sigma) = T$ então α vale em todo modelo de Σ. Logo todo modelo de Σ é também modelo de T:

$$Ded_{\mathcal{L}}(\Sigma) = T \Rightarrow Mod_{\mathcal{L}}(\Sigma) \subset Mod_{\mathcal{L}}(T)$$

A inclusão contrária é amparada pelo Teorema 4.4.13, e portanto

$$Ded_{\mathcal{L}}(\Sigma) = T \Rightarrow Mod_{\mathcal{L}}(\Sigma) = Mod_{\mathcal{L}}(T)$$

O caso mais interessante de axiomatização de uma $\mathcal{L}$-teoria $Th_{\mathcal{L}}(M)$ (isto é, a busca por um sistema de axiomas para ela) acontece quando M tem apenas um elemento. De fato, note que, neste caso, o conjunto

$$Th_{\mathcal{L}}(\mathfrak{A}) = \{\alpha \in Sent_{\mathcal{L}} \mid \mathfrak{A} \models \alpha\}$$

tem a seguinte propriedade: para cada $\alpha \in Sent_{\mathcal{L}}$, tem-se

$$\text{ou} \quad \mathfrak{A} \models \alpha \quad \text{ou} \quad \mathfrak{A} \models \neg\alpha,$$

ou seja,

$$\text{ou} \quad \alpha \in Th_{\mathcal{L}}(\mathfrak{A}) \quad \text{ou} \quad \neg\alpha \in Th_{\mathcal{L}}(\mathfrak{A}).$$

No entanto, se M não é unitário, então não podemos afirmar que, para cada $\alpha \in Sent_{\mathcal{L}}$, tem-se

$$\text{ou} \quad \alpha \in Th_{\mathcal{L}}(M) \quad \text{ou} \quad \neg\alpha \in Th_{\mathcal{L}}(M).$$

Exemplo 4.5.7 *Na linguagem de anéis (veja Exemplo 4.1.4) considere as $\mathcal{L}$-estruturas $\boldsymbol{Z}$ e $\boldsymbol{Q}$, onde $|\boldsymbol{Z}| = \mathbb{Z}$ e $|\boldsymbol{Q}| = \mathbb{Q}$. Vemos que se tomamos $M = \{\boldsymbol{Z}, \boldsymbol{Q}\}$ então para a sentença α:*

$$\forall x(\neg x \doteq 0 \rightarrow \exists y \;\; xy \doteq 1).$$

temos que,

$$\alpha \notin Th_{\mathcal{L}}(M) \quad e \quad \neg\alpha \notin Th_{\mathcal{L}}(M).$$

Este fato nos sugere a seguinte

Definição 4.5.8 *Dizemos que uma teoria T é completa se, para cada $\alpha \in Sent_{\mathcal{L}}$, tem-se*

$$ou \quad \alpha \in T \quad ou \quad \neg\alpha \in T.$$

Com esta definição vemos que dada uma $\mathcal{L}$-estrutura $\mathfrak{A}$, a teoria $Th_{\mathcal{L}}(\mathfrak{A})$ é sempre completa.

Obviamente, se Σ é um sistema de axiomas para uma teoria completa T, então Σ satisfaz

$$\text{ou} \quad \Sigma \vdash \alpha \quad \text{ou} \quad \Sigma \vdash \neg\alpha,$$

para cada $\alpha \in Sent_{\mathcal{L}}$.

Isto nos leva à seguinte definição mais geral:

Definição 4.5.9 *Dizemos que $\Sigma \in Sent_{\mathcal{L}}$ é um sistema de axiomas completo, se, para cada $\alpha \in Sent_{\mathcal{L}}$, tem-se*

$$ou \quad \Sigma \vdash \alpha \quad ou \quad \Sigma \vdash \neg\alpha. \tag{82}$$

Salientamos que, se Σ é um sistema de axiomas para uma teoria T, isto é, $T = Ded_{\mathcal{L}}(\Sigma)$, então T é uma teoria completa se, e somente se, Σ é um sistema de axiomas completo.

A importância da teoria $Th_{\mathcal{L}}(\mathfrak{A})$ segue do seguinte fato: se $\Sigma \subset Sent_{\mathcal{L}}$ é um sistema de axiomas completo e $\mathfrak{A}$ é um modelo de Σ então vale

$$Th_{\mathcal{L}}(\mathfrak{A}) = Ded_{\mathcal{L}}(\Sigma).$$

Ou seja, $Ded_{\mathcal{L}}(\Sigma)$ é a teoria da $\mathcal{L}$-estrutura $\mathfrak{A}$. Assim, se Σ é um sistema de axiomas de uma Teoria completa T, então

$$T = Th_{\mathcal{L}}(\mathfrak{A}),$$

para todo modelo $\mathfrak{A}$ de Σ. Para isto, basta observar que sendo $\mathfrak{A}$ um modelo de Σ, vale $\Sigma \subset Th_{\mathcal{L}}(\mathfrak{A})$ e com isto $Ded_{\mathcal{L}}(\Sigma) \subset Th_{\mathcal{L}}(\mathfrak{A})$ pelo Teorema 4.4.13.

A igualdade acima mencionada segue então do fato das teorias $Ded_{\mathcal{L}}(\Sigma)$ e $Th_{\mathcal{L}}(\mathfrak{A})$ serem completas (veja Teorema 4.4.14) e do seguinte Lema.

Lema 4.5.10 *Se T_1 e T_2 são $\mathcal{L}$-teorias completas com $T_1 \subset T_2$, então vale $T_1 = T_2$.*

Prova. Se existe $\alpha \in T_2$ com $\alpha \notin T_1$, então de T_1 ser completa segue que $\neg\alpha \in T_1$, e com isto $\neg\alpha \in T_2$, o que contradiz a não contraditoriedade de T_2.

■

Exemplo 4.5.11 *Vejamos alguns exemplos de sistemas de axiomas para as linguagens que apresentamos no Exemplo 4.1.4:*

(1) ***Um sistema de axiomas para grupos abelianos totalmente***

***ordenados**: Consideramos os seguintes axiomas:*

O_1 : $\forall x\ \neg(x < x)$; *(antisimetria)*

O_2 : $\forall x, y, z\ ((x < y \wedge y < z \rightarrow x < z))$; *(transitividade)*

O_3 : $\forall x, y\ (x < y \vee x \doteq y \vee y < x)$; *(ordem total)*

G_1 : $\forall x, y, z\ ((x + y) + z) \doteq (x + (y + z))$; *(associatividade)*

G_2 : $\forall x\ x + 0 \doteq x$; *(axioma do elemento neutro)*

G_3 : $\forall x\ \exists y\ x + y \doteq 0$; *(inverso aditivo)*

G_4 : $\forall x, y\ x + y \doteq y + x$; *(comutatividade)*

OG : $\forall x, y, z\ (x < y \rightarrow x + z < y + z)$; *(axioma de compatibilidade)*

O sistema de axiomas para grupos abelianos totalmente ordenados e não triviais é o conjunto

$$\Sigma = \{O_1, O_2, O_3, G_1, G_2, G_3, G_4, OG\} \cup \{\exists x\ x \neq 0\}.$$

(compare com a Definição 3.3.1).

(2) ***Um sistema de axiomas***

(*a*) ***para corpos:***

K_0 : $0 \neq 1$;

K_1 : $\forall x, y, z\ \ x + (y + z) \doteq (x + y) + z$;
(associatividade da soma)

K_2 : $\forall x\ x + 0 \doteq x$;
(elemento neutro para soma)

K_3 : $\forall x \exists y\ \ x + y \doteq 0$;
(inverso aditivo)

K_4 : $\forall x, y\ \ x + y = y + x$
(comutatividade da soma)

K_5 : $\forall x, y, z\ \ x.(y.z) \doteq (x.y).z$;
(associatividade da multiplicação)

K_6 : $\forall x\ x.1 \doteq x$;
(elemento neutro da multiplicação)
K_7 : $\forall x\ \exists y\ (x \doteq 0 \vee x.y \doteq 1)$;
(inverso multiplicativo)
K_8 : $\forall x, y\ \ x.y \doteq y.x$;
(comutatividade da multiplicação)
K_9 : $\forall x, y, z\ \ (x + y).z \doteq x.z + y.z$;
(lei distributiva)

(b) ***para anéis:*** *Retirando a sentença do inverso multiplicativo e da comutatividade temos um sistema de axiomas para anéis com unidade.*

(c) ***para corpos ordenados:*** *Podemos ainda estudar uma ordem neste corpo, ou seja, adicionar à nossa lista $O_1 - O_3, OG$ e também o seguinte axioma.*

$$OK\ :\ \forall x, y\ (0 < x \wedge 0 < y\ \rightarrow\ 0 < x.y).$$

(3) ***Um sistema de axiomas para corpos valorizados:*** *Podemos achar um sistema de axiomas para corpos valorizados adicionando ao conjunto de axiomas de corpos os seguintes axiomas:*

V_1 : $V(0) \wedge V(1)$;
V_2 : $\forall x, y\ (V(x) \wedge V(y)\ \rightarrow\ V(x - y) \wedge V(x.y))$;
V_3 : $\forall x, y\ (\ (x.y) = 1\ \rightarrow\ V(x) \vee V(y)\ )$;

No que segue, denotaremos um modelo de $\Sigma = \{K_0 - K_9, V_1 - V_3\}$ resumidamente por $(F, \mathcal{O})$, onde F é o corpo determinado por este modelo e $\mathcal{O}$ é o anel de valorização de F determinado pela interpretação de V nesta estrutura. Mais precisamente, se $\mathfrak{A}$ é tal modelo. $|\mathfrak{A}| = F$ e

$$\mathcal{O} = \{t^{\mathfrak{A}}[h] \mid \mathfrak{A} \models V(t)[h] \text{ para alguma avaliação } h \text{ em } \mathfrak{A} \text{ e } t \text{ termo}\}$$

(4) ***Um sistema de axiomas para corpos valorizados henselianos:***

Neste caso acrescentamos aos axiomas $K_0 - K_9$ e $V_1 - V_3$, para cada grau $n \geq 2$, os axiomas H_n que exprimem a condição (4) do Teorema 3.6.4. Para isto, se f é um polinômio mônico de grau n, a saber,

$$f = X^n + x_{n-1}X^{n-1} + ... + x_0,$$

escrevemos resumidamente $(\forall f \in V[X])\varphi$ e $\psi(f(y))$ em H_n, para $\forall x_0, ..., x_{n-1}\ (\bigwedge_{i=0}^{n-1} V(x_i) \rightarrow \varphi)$ e $\psi(y^n + x_{n-1}y^{n-1} + ... + x_0)$, respectivamente. Também escrevemos f' para a derivada de f definida por:

$$nX^{n-1} + (n-1)x_{n-1}X^{n-2} + ... + x_1$$

E por fim, definimos $V^\times(z)$ como sendo a fórmula

$$V(z) \wedge \exists y\ (yz \doteq 1 \wedge V(y)),$$

a qual determina as unidades em um anel de valorização . Definimos portanto para cada $n \in \mathbb{N}$:

$$\begin{aligned} H_n\ : (\forall f \in V[X])\ \forall y\ (&\neg V^\times(f(y)) \wedge V^\times(f'(y)) \wedge V(y) \\ &\rightarrow \exists z\ (V(z) \wedge f(z) \doteq 0 \wedge \neg V^\times(y - z))) \end{aligned}$$

Assim, um corpo henseliano é então um modelo de

$$\Sigma = \{K_0 - K_9, V_1 - V_3\} \cup \{H_n \mid n \in \mathbb{N}\}.$$

4.6 Construção de Modelos

O objetivo desta seção é provar que se um conjunto $\Sigma \subset Sent_{\mathcal{L}}$ possui um modelo de cardinalidade infinita, então possui também um modelo de cardinalidade κ para cada número cardinal κ suficientemente grande. Para tal, precisamos definir cardinalidade de uma linguagem e de um modelo.

Definição 4.6.1 *Dada uma linguagem $\mathcal{L} = (\lambda, \mu, K)$, definimos a cardinalidade de $\mathcal{L}$ pelo cardinal*

$$\kappa_{\mathcal{L}} := \max(\aleph_0, \mathsf{card}(I), \mathsf{card}(J), \mathsf{card}(K)).$$

Salientamos que, como tratado na seção 4.1, o alfabeto de uma linguagem formal de primeira ordem é constituído por símbolos lógicos ($\neg$, $\wedge$, $\forall$, $\doteq$), variáveis ($v_0, ..., v_n, ...$, com $n \in \mathbb{N}$), símbolos relacionais (R_i, com $i \in I$), símbolos funcionais (f_j, com $j \in J$), símbolos constantes (c_k, com $k \in K$) e símbolos auxiliares (quatro apenas), de modo que seria natural definirmos como cardinalidade de uma liguagem a cardinalidade do conjunto união

$$\mathbb{N} \cup I \cup J \cup K \cup \{\ .\ ;\ )\ ;\ (\ ;\ ,\ ;\ \neg\ ;\ \wedge\ ;\ \forall\ ;\ \doteq\ \}.$$

Porém, como já temos uma cardinalidade infinita ($\aleph_0$ =$\mathsf{card}(\mathbb{N})$), esta cardinalidade é dada precisamente por

$$\max(\aleph_0, \mathsf{card}(I), \mathsf{card}(J), \mathsf{card}(K)),$$

de modo que a definição acima é completamente natural.

Definição 4.6.2 *Se $\mathfrak{A}$ é uma $\mathcal{L}$-estrutura, então denominamos cardinalidade de $\mathfrak{A}$ como sendo a cardinalidade de seu domínio $|\mathfrak{A}|$.*

O objetivo desta seção é provar o seguinte teorema

Teorema 4.6.3 *Se $\Sigma \subset Sent_{\mathcal{L}}$ possui um modelo de cardinalidade infinita, então possui um modelo de cardinalidade κ para cada número cardinal $\kappa \geq \kappa_{\mathcal{L}}$.*

Antes de prová-lo, calculamos algumas cardinalidades.

Se uma linguagem $\mathcal{L} = (\lambda, \mu, K)$ tem funções aridades $\lambda : I \to \mathbb{N}$ e $\mu : J \to \mathbb{N}$ então:

$$\mathsf{card}(Tm_{\mathcal{L}}) = \max(\aleph_0, \mathsf{card}(J), \mathsf{card}(K)) \tag{83}$$

$$\mathsf{card}(Sent_{\mathcal{L}}) = \mathsf{card}(Fml_{\mathcal{L}}) = \kappa_{\mathcal{L}}. \tag{84}$$

Isto segue do fato conhecido de que o conjunto de todas as seqüências finitas com valores em um conjunto infinito M tem a mesma cardinalidade que M. Para (83), levando em conta a Definição 4.1.2, concluímos que todo termo é uma seqüência finita de símbolos do conjunto

$$M = Vbl \cup \{f_j \mid i \in J\} \cup \{c_k \mid k \in K\} \cup \{\ )\ ,\ (\ \},$$

cuja cardinalidade é exatamente

$$\max(\aleph_0, \mathsf{card}(J), \mathsf{card}(K)),$$

donde segue que

$$\mathsf{card}(Tm_{\mathcal{L}}) \leq \mathsf{card}(M).$$

Por outro lado v_n, c_k e $f_j(v_0, ..., v_0)$ são termos para cada $j \in J$, $k \in K$ e $n \in \mathbb{N}$, donde obtemos uma função injetiva de M em $Tm_{\mathcal{L}}$, e portanto

$$\mathsf{card}(M) \leq \mathsf{card}(Tm_{\mathcal{L}}).$$

Daí segue a igualdade das cardinalidades.

Para provar (84), levando em conta a Definição 4.1.3, concluímos que toda fórmula é uma seqüência finita de símbolos do conjunto

$$M := Tm_{\mathcal{L}} \cup \{R_i \mid i \in I\} \cup \{\neg\ \wedge\ \forall\ \doteq\ )\ ,\ (\ \}$$

cuja cardinalidade é exatamente $\kappa_{\mathcal{L}}$, pois é igual a

$$\max(\mathsf{card}(Tm_{\mathcal{L}}), \mathsf{card}(I)) = \max(\aleph_0, \mathsf{card}(I), \mathsf{card}(J), \mathsf{card}(K)) = \kappa_{\mathcal{L}},$$

e portanto

$$\mathsf{card}(Fml_{\mathcal{L}}) \leq \kappa_{\mathcal{L}}$$

E, como $Sent_{\mathcal{L}} \subset Fml_{\mathcal{L}}$, obtém-se

$$\mathsf{card}(Sent_{\mathcal{L}}) \leq \mathsf{card}(Fml_{\mathcal{L}}) \leq \kappa_{\mathcal{L}}.$$

Por outro lado

$$t \doteq t \quad \text{e} \quad \forall v_0 \; R_i(v_0, ..., v_0)$$

são $\mathcal{L}$-sentenças para todo $t \in Tm_{\mathcal{L}}$ e todo $i \in I$, donde claramente obtemos uma função injetiva de M em $Sent_{\mathcal{L}}$, e portanto vale também

$$\kappa_{\mathcal{L}} \leq \mathsf{card}(Sent_{\mathcal{L}}),$$

donde obtemos

$$\mathsf{card}(Sent_{\mathcal{L}}) = \mathsf{card}(Fml_{\mathcal{L}}) = \kappa_{\mathcal{L}}.$$

A partir destas observações estimamos a cardinalidade do conjunto

$$A = TC/\approx .$$

Temos, naturalmente,

$$\mathsf{card}(TC/\approx) \leq \mathsf{card}(TC) \leq \mathsf{card}(Tm_{\mathcal{L}'}) \leq \kappa_{\mathcal{L}'}. \tag{85}$$

Afirmamos agora que

$$\kappa_{\mathcal{L}'} = \kappa_{\mathcal{L}}. \tag{86}$$

De fato, lembramos que a linguagem $\mathcal{L}'$ foi construída na prova do Teorema 4.3.5 como a união de uma cadeia ascendente

$$\mathcal{L} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset ... \subset \mathcal{L}_{n-1} \subset \mathcal{L}_n \subset ... \tag{87}$$

Vamos mostrar por indução, que $\kappa_{\mathcal{L}_n} \leq \kappa_{\mathcal{L}}$, para todo n, pois daí segue que

$$\kappa_{\mathcal{L}'} \leq \kappa_{\mathcal{L}},$$

e como

$$\kappa_{\mathcal{L}} = \kappa_{\mathcal{L}_0} \leq \kappa_{\mathcal{L}'},$$

obtemos $\kappa_{\mathcal{L}'} = \kappa_{\mathcal{L}}$.

Para $n = 0$ é trivial. Suponhamos $n \geq 1$ e que $\kappa_{\mathcal{L}_{n-1}} \leq \kappa_{\mathcal{L}}$. Em particular, da construção da cadeia (87) no Teorema 4.3.5, sabemos que a linguagem $\mathcal{L}_n$ resulta de $\mathcal{L}_{n-1}$ por um aumento do conjunto de índices K_{n-1} por um conjunto $\underline{K_{n-1}}$, o qual tem a cardinalidade igual a de um subconjunto de $Sent_{\mathcal{L}_{n-1}}$. Como

$$\mathsf{card}(Sent_{\mathcal{L}_{n-1}}) \overset{(84)}{=} \kappa_{\mathcal{L}_{n-1}},$$

temos $\mathsf{card}(\underline{K_{n-1}}) \leq \kappa_{\mathcal{L}_{n-1}}$. Assim, vale:

$$\begin{array}{rcl} \kappa_{\mathcal{L}_n} & \overset{Def.\ 4.6.1}{=} & \max\{\aleph_0, \mathsf{card}(I), \mathsf{card}(J), \mathsf{card}(K_{n-1} \cup \underline{K_{n-1}})\} \\ & \leq & \max(\kappa_{\mathcal{L}_{n-1}},\ \mathsf{card}(\underline{K_{n-1}})) \\ & = & \kappa_{\mathcal{L}_{n-1}} \\ & \leq & \kappa_{\mathcal{L}}\ . \end{array}$$

Agora estamos em condições de provar o teorema enunciado anteriormente:

Prova.[Prova do Teorema 4.6.3] Fixado um número cardinal $\kappa \geq \kappa_{\mathcal{L}}$, definimos uma extensão $\mathcal{L}_\kappa$ da linguagem $\mathcal{L}$ pondo

$$I_\kappa = I\ ,\ J_\kappa = J\ ,\ K_\kappa = K \cup \{\nu \mid \nu < \kappa\},$$

onde supomos, sem perda de generalidade, que a última união é disjunta.

Uma $\mathcal{L}_\kappa$-estrutura é assim uma $\mathcal{L}$-estrutura, para a qual ainda acrescentamos interpretações para as constantes c_ν para $\nu < \kappa$.

Na linguagem $\mathcal{L}_\kappa$ consideramos o seguinte conjunto de sentenças:

$$\Sigma_\kappa := \Sigma \cup \{c_\nu \neq c_\mu \mid \nu < \mu < \kappa\}.$$

Afirmamos que este conjunto é não-contraditório, e para ver isto, pelo Corolário 4.4.14, basta mostrar que Σ_κ admite um modelo. E, por sua vez,

pelo Teorema 4.4.15, basta mostrar que cada subconjunto finito Φ de Σ_κ admite um modelo. Ora, cada subconjunto finito Φ de Σ_κ está contido em algum conjunto da forma

$$\Sigma \cup \{c_{\nu_1} \neq c_{\mu_1}, ..., c_{\nu_n} \neq c_{\mu_n}\}$$

para núneros ordinais $\nu_i < \mu_i < \kappa$ com $1 \leq i \leq n$. Este conjunto contudo possui um modelo, pois pela hipótese Σ possui um modelo $\mathfrak{A}$ infinito. Para ver isto, basta dar interpretações para as novas constantes c_ν com $\nu < \kappa$, de tal forma que, para $1 \leq i \leq n$, as constantes c_{ν_i} e c_{μ_i} tenham interpretações distintas, o que é possível em $\mathfrak{A}$. Assim, Σ_κ admite um modelo.

Para mostrarmos que Σ admite um modelo de cardinalidade κ, consideramos a estrutura $\mathfrak{A}'$ que foi utilizada no Teorema 4.4.10 e cujo domínio foi construído na seção 4.3 para a linguagem $\mathcal{L}_\kappa$. Sabemos então que $\mathfrak{A}'$ é uma $\mathcal{L}$-estrutura com adicionais interpretações das constantes c_ν para $\nu < \kappa$ e das constantes que aparecem da transição de $\mathcal{L}_\kappa$ para $\mathcal{L}'$. A restrição $\mathfrak{B}$ de $\mathfrak{A}'$ sobre a linguagem $\mathcal{L}_\kappa$, a qual obtemos ignorando as interpretações de constantes adicionais, é evidentemente um modelo de Σ_κ e portanto também para Σ. Afirmamos que $|\mathfrak{B}| = |\mathfrak{A}'|$ tem cardinalidade κ.

De fato, $\mathfrak{A}'$ é sem dúvida um modelo para $\{c_\mu \neq c_\mu \mid \nu < \mu < \kappa\}$. As interpretações das constantes nos fornecem uma injeção $c_\nu \mapsto c_\nu^{\mathfrak{A}'}$ de $\{c_\nu \mid \nu < \kappa\}$ em $|\mathfrak{A}'|$, e com isto também uma injeção do conjunto

$$\{\nu \mid \nu < \kappa\}$$

em $|\mathfrak{A}'|$. Assim vale

$$\kappa = \mathsf{card}(\{\nu \mid \nu < \kappa\}) \leq \mathsf{card}(|\mathfrak{B}|). \tag{88}$$

Por outro lado, por (85), a cardinalidade de $\mathfrak{A}'$ é limitada por cima pela cardinalidade da linguagem $\mathcal{L}_{\kappa'}$ que, por (86), é igual a $\mathsf{card}(\mathcal{L}_\kappa)$.

Assim, vale

$$\begin{aligned} \mathsf{card}(|\mathfrak{B}|) &\leq \mathsf{card}(|\mathfrak{A}'|) \\ &\leq \mathsf{card}(\mathcal{L}_\kappa) \\ &= \max\{\aleph_0, \mathsf{card}(I), \mathsf{card}(J), \mathsf{card}(K \cup \{\nu \mid \nu < \kappa\})\} \\ &\leq \max\{\kappa_{\mathcal{L}}, \kappa\} \leq \kappa, \end{aligned}$$

sendo que a última desigualdade é válida pela hipótese $\kappa \geq \kappa_{\mathcal{L}}$.

Daqui e de (88) segue

$$\mathsf{card}(|\mathfrak{B}|) = \kappa,$$

o que completa a prova.

■

Definição 4.6.4 *Dizemos que duas $\mathcal{L}$-estruturas $\mathfrak{A}$ e $\mathfrak{A}'$ são elementarmente equivalentes se, para toda $\mathcal{L}$-sentença φ,*

$$\mathfrak{A} \models \varphi \quad \textit{implica} \quad \mathfrak{A}' \models \varphi$$

e escreveremos $\mathfrak{A} \equiv \mathfrak{A}'$ para denotar este fato.

Afirmamos que $\equiv$ é uma relação de equivalência na classe de todas as $\mathcal{L}$-estruturas. De fato, note, por exemplo, que

não é verdade que $\mathfrak{A} \models \varphi$ se e só se
$\mathfrak{A} \not\models \varphi$ se e só se (veja Definição 4.4.5, (3))
$\mathfrak{A} \models \neg\varphi$ implica, pela definição de $\equiv$,
$\mathfrak{A}' \models \neg\varphi$ se e só se
$\mathfrak{A}' \not\models \varphi$ se e só se
não é verdade que $\mathfrak{A}' \models \varphi$,

o que prova a simetria da relação $\equiv$.

Do Teorema 4.6.3 obtemos que as classes de equivalência da relação $\equiv$ que possuem uma $\mathcal{L}$-estrutura infinita, possuem estruturas de cardinalidade arbitrariamente grande. Para verificar isto consideramos o conjunto

da $\mathcal{L}$-teoria de uma estrutura $\mathfrak{A}$,

$$Th_{\mathcal{L}}(\mathfrak{A}) := \{\varphi \in Sent_{\mathcal{L}} \mid \mathfrak{A} \models \varphi\},$$

observamos que um modelo $\mathfrak{B}$ de $Th_{\mathcal{L}}(\mathfrak{A})$ é elementarmente equivalente a $\mathfrak{A}$. De fato, se

$$\mathfrak{A} \models \varphi$$

temos $\varphi \in Th_{\mathcal{L}}(\mathfrak{A})$, e portanto

$$\mathfrak{B} \models \varphi.$$

Empregando o Teorema 4.6.3 sobre o conjunto $\Sigma = Th_{\mathcal{L}}(\mathfrak{A})$ obtemos precisamente que

Corolário 4.6.5 *Para cada $\mathcal{L}$-estrutura $\mathfrak{A}$ de cardinalidade infinita, e cada número cardinal $\kappa \geq \kappa_{\mathcal{L}}$ existe uma $\mathcal{L}$-estrutura $\mathfrak{B}$ elementarmente equivalente a $\mathfrak{A}$ e que tem cardinalidade κ.*

O corolário acima nos garante que nenhuma $\mathcal{L}$-estrutura infinita de um sistema de axiomas $\Sigma \subset Sent_{\mathcal{L}}$ pode ser caracterizada por isomorfismos. Explicamos os detalhes desta afirmação na próxima seção.

4.7 Morfismos de estruturas

Definição 4.7.1 *Dizemos que uma aplicação $\tau : |\mathfrak{A}| \to |\mathfrak{A}'|$ entre os domínios de duas $\mathcal{L}$-estruturas $\mathfrak{A}$ e $\mathfrak{A}'$ é um:*

- $\mathcal{L}$-morfismo entre $\mathfrak{A}$ e $\mathfrak{A}'$ quando as seguintes condições são satisfeitas:

(I_1) $\tau(f_j^{\mathfrak{A}}(a_1, ..., a_{\mu(j)})) = f_j^{\mathfrak{A}'}(\tau(a_1), ..., \tau(a_{\mu(j)}))$ *para todo $j \in J$ e todo $a_1, ..., a_{\mu(j)} \in |\mathfrak{A}|$,*

(I_2) $R_i^{\mathfrak{A}}(a_1, ..., a_{\lambda(i)})$ *sse* $R_i^{\mathfrak{A}'}(\tau(a_1), ..., \tau(a_{\lambda(i)}))$ *para todo $i \in I$ e todo $a_1, ..., a_{\lambda(i)} \in |\mathfrak{A}|$,*

(I_3) $\tau(c_k^{\mathfrak{A}}) = c_k^{\mathfrak{A}'}$ *para todo $k \in K$.*

- $\mathcal{L}$-isomorfismo entre $\mathfrak{A}$ e $\mathfrak{A}'$ quando τ é, além de morfismo, uma bijeção,

e neste caso escrevemos resumidamente

$$\tau : \mathfrak{A} \leftrightarrow \mathfrak{A}' \quad \textit{ou apenas} \quad \mathfrak{A} \simeq \mathfrak{A}',$$

quando a especificação da função τ não for relevante;

- *$\mathcal{L}$-automorfismo de $\mathfrak{A}$ quando τ é um $\mathcal{L}$-isomorfismo de $\mathfrak{A}$ em $\mathfrak{A}$;*

- *$\mathcal{L}$-monomorfismo entre $\mathfrak{A}$ e $\mathfrak{A}'$ ou $\mathcal{L}$-imersão de $\mathfrak{A}$ em $\mathfrak{A}'$ quando τ é, além de morfismo, uma aplicação injetora, e neste caso escrevemos resumidamente*

$$\tau : \mathfrak{A} \rightarrowtail \mathfrak{A}' \quad \textit{ou apenas} \quad \mathfrak{A} \hookrightarrow \mathfrak{A}',$$

quando a especificação da função τ não for relevante.

Observação 4.7.2 *Para aplicações posteriores, observamos que as condições (I_1) e (I_3) são equivalentes às condições*

(I_1') $f_j^{\mathfrak{A}}(a_1, ..., a_{\mu(j)}) = d$ *implica* $f_j^{\mathfrak{A}'}(\tau(a_1), ..., \tau(a_{\mu(j)})) = \tau(d)$ *para todo* $j \in J$ *e* $a_1, ..., a_{\mu(j)}, d \in |\mathfrak{A}|$,

(I_3') $c_k^{\mathfrak{A}} = d$ *implica* $c_k^{\mathfrak{A}'} = \tau(d)$ *para todo* $k \in K$ *e* $d \in |\mathfrak{A}|$,

escritas na forma de implicação.

Teorema 4.7.3 *Sejam $\mathfrak{A}$ e $\mathfrak{A}'$ duas $\mathcal{L}$-estruturas e $\tau : \mathfrak{A} \leftrightarrow \mathfrak{A}'$ um isomorfismo entre elas. Então, para cada $\mathcal{L}$-fórmula φ e cada avaliação h em $\mathfrak{A}$,*

$$\mathfrak{A} \models \varphi[h] \quad \textit{se e só se} \quad \mathfrak{A}' \models \varphi[\tau \circ h];$$

em particular, $\mathfrak{A}$ e $\mathfrak{A}'$ são elementarmente equivalentes.

Prova. Inicialmente salientamos que se h é uma avaliação em $|\mathfrak{A}|$, então é claro que $h' = \tau \circ h$ é uma avaliação em $|\mathfrak{A}'|$.

A seguir, mostramos que, para cada termo $t \in Tm_{\mathcal{L}}$ temos

$$\tau(t^{\mathfrak{A}}[h]) = t^{\mathfrak{A}'}[h'], \tag{89}$$

fazendo uso de indução sobre a sua construção:

- Para constantes c_k esta condição é exatamente a condição (I_3);

- Para uma variável x, temos

$$\tau(x^{\mathfrak{A}}[h]) = \tau(h(x)) = h'(x) = x^{\mathfrak{A}'}[h'];$$

- Para um termo da forma $f_j(t_1, ..., t_{\mu(j)})$ segue, pela hipótese de indução e pela condição (I_1):

$$\begin{aligned}\tau(f_j(t_1, ..., t_{\mu(j)}))^{\mathfrak{A}}[h]) &= \tau(f_j^{\mathfrak{A}}(t_1^{\mathfrak{A}}[h], ..., t_{\mu(j)}^{\mathfrak{A}}[h])) \\ &= f_j^{\mathfrak{A}'}(\tau(t_1^{\mathfrak{A}})[h], ..., \tau(t_{\mu(j)}^{\mathfrak{A}})[h]) \\ &= f_j^{\mathfrak{A}'}(t_1^{\mathfrak{A}'}[h'], ..., t_{\mu(j)}^{\mathfrak{A}'}[h']) \\ &= f_j(t_1, ..., t_{\mu(j)})^{\mathfrak{A}'}[h'].\end{aligned}$$

Podemos agora mostrar a equivalência

$$\mathfrak{A} \models \varphi[h] \text{ se e só se } \mathfrak{A}' \models \varphi[h'],$$

por indução sobre a construção da fórmula φ:

- Para uma fórmula atômica do tipo $t_1 \doteq t_2$ obtemos, pela injetividade de τ,

$$\begin{aligned}&\mathfrak{A} \models (t_1 \doteq t_2)[h] \text{ se e só se} \\ &\quad t_1^{\mathfrak{A}}[h] = t_2^{\mathfrak{A}}[h] \text{ se e só se} \\ &\quad \tau(t_1^{\mathfrak{A}}[h]) = \tau(t_2^{\mathfrak{A}}[h]) \text{ se e só se (por (89))} \\ &\quad t_1^{\mathfrak{A}'}[h'] = t_2^{\mathfrak{A}'}[h'] \text{ se e só se} \\ &\mathfrak{A}' \models (t_1 \doteq t_2)[h'].\end{aligned}$$

- Para uma fórmula atômica do tipo $R_i(t_1, ..., t_{\lambda(i)})$ obtemos, por (I_2) :

$$\begin{aligned}&\mathfrak{A} \models R_i(t_1, ..., t_{\lambda(i)})[h] \text{ se e só se} \\ &\quad R_i^{\mathfrak{A}}(t_1^{\mathfrak{A}}[h], ..., t_{\lambda(i)}^{\mathfrak{A}}[h]) \text{ se e só se} \\ &\quad R_i^{\mathfrak{A}'}(\tau(t_1^{\mathfrak{A}}[h]), ..., \tau(t_{\lambda(i)}^{\mathfrak{A}}[h])) \text{ se e só se (por (89))} \\ &\quad R_i^{\mathfrak{A}'}(t_1^{\mathfrak{A}'}[h'], ..., t_{\lambda(i)}^{\mathfrak{A}'}[h']) \text{ se e só se} \\ &\mathfrak{A}' \models R_i(t_1, ..., t_{\lambda(i)})[h'].\end{aligned}$$

- Para uma fórmula do tipo $\neg\psi$ obtemos, pela hipótese de indução:

$$\begin{aligned}
&\mathfrak{A} \models \neg\psi[h] \text{ se e só se}\\
&\mathfrak{A} \not\models \psi[h] \text{ se e só se (pela hipótese de indução)}\\
&\mathfrak{A}' \not\models \psi[h'] \text{ se e só se}\\
&\mathfrak{A}' \models \neg\psi[h'].
\end{aligned}$$

- Para uma fórmula do tipo $(\psi_1 \wedge \psi_2)$ obtemos, pela hipótese de indução:

$$\begin{aligned}
&\mathfrak{A} \models (\psi_1 \wedge \psi_2)[h] \text{ se e só se}\\
&(\mathfrak{A} \models \psi_1[h] \text{ e } \mathfrak{A} \models \psi_2[h]) \text{ se e só se}\\
&(\mathfrak{A}' \models \psi_1[h'] \text{ e } \mathfrak{A}' \models \psi_2[h']) \text{ se e só se}\\
&(\mathfrak{A}' \models (\psi_1 \wedge \psi_2)[h']).
\end{aligned}$$

- No caso de uma fórmula do tipo $\forall x\psi$, obtemos, pela hipótese de indução sobre a fórmula ψ, pelas avaliações $h(x,a)$ para $a \in |\mathfrak{A}|$ e pela sobrejetividade[7] de τ:

$$\begin{aligned}
&\mathfrak{A} \models \forall x\ \psi[h] \text{ se e só se}\\
&\mathfrak{A} \models \psi[h(x,a)] \text{ para todo } a \in |\mathfrak{A}| \text{ se e só se (pela hipótese de indução)}\\
&\mathfrak{A}' \models \psi[\tau \circ (h(x,a))] \text{ para todo } a \in |\mathfrak{A}| \text{ se e só se}\\
&\mathfrak{A}' \models \psi[h'(x,\tau(a))] \text{ para todo } a \in |\mathfrak{A}| \text{ se e só se}\\
&\mathfrak{A}' \models \psi[h'(x,a')] \text{ para todo } a' \in |\mathfrak{A}'| \text{ se e só se}\\
&\mathfrak{A}' \models \forall x\ \psi[h'].
\end{aligned}$$

Salientamos que, por causa da sobrejetividade de τ, podemos colocar $\tau(a) = a'$ para todo $a' \in |\mathfrak{A}'|$ e para algum $a \in |\mathfrak{A}|$.

A afirmação

$$\mathfrak{A} \equiv \mathfrak{A}'$$

[7]Salientamos que aqui é a primeira vez nesta demonstração em que está sendo utilizada a sobrejetividade de τ. Faremos alusão a esta observação no Corolário 4.7.4 e no Lema 4.8.7.

é garantida empregando-se para as $\mathcal{L}$-sentenças as equivalências que acabamos de provar.

■

Com isto mostramos, para duas $\mathcal{L}$-estruturas $\mathfrak{A}$ e $\mathfrak{A}'$, que

$$\mathfrak{A} \simeq \mathfrak{A}' \quad \text{implica} \quad \mathfrak{A} \equiv \mathfrak{A}'. \tag{90}$$

Observamos que não vale a recíproca do resultado acima: de fato, na seção anterior mostramos que se uma teoria admite um modelo de cardinalidade infinita então admite um modelo de cardina- lidade infinita arbitrária. Ora, todos os modelos de $Th(\mathfrak{A})$ são elementarmente equivalentes, mas obviamente dois modelos de cardinalidade diferente não são isomorfos. Fica assim explicada a última frase da seção anterior.

O Teorema 4.7.5 a seguir estabelece condições que garantem a recíproca da implicação (90).

Começamos com um Corolário da prova do Teorema 4.7.3:

Corolário 4.7.4 *Se uma aplicação $\tau : |\mathfrak{A}| \to |\mathfrak{A}'|$ é um monomorfismo de $\mathfrak{A}$ em $\mathfrak{A}'$, então vale, para toda fórmula φ sem quantificadores e para toda avaliação h em $\mathfrak{A}$:*

$$\mathfrak{A} \models \varphi[h] \quad \textit{se e só se} \quad \mathfrak{A}' \models \varphi[\tau \circ h] \tag{91}$$

Reciprocamente, se esta equivalência vale para toda fórmula φ sem quantificadores e para toda avaliação h em $\mathfrak{A}$, então τ é um monomorfismo de $\mathfrak{A}$ em $\mathfrak{A}'$.

Prova. Na prova do Teorema 4.7.3, a sobrejetividade de τ foi usada apenas no caso de uma fórmula quantificada do tipo $\forall\, x\ \psi$, e portanto é claro que a equivalência (91) vale para toda fórmula na qual nenhum quantificador do tipo $\forall\, x$ foi utilizado.

Para provar a recíproca, suponhamos que vale (91) para qualquer avaliação h e qualquer fórmula sem quantificadores. Em particular, para qualquer avaliação h nas fórmulas

$$R_i(v_1, ..., v_{\lambda(i)}), \text{ para } i \in I,$$

$$f_j(v_1, ..., v_{\mu(j)}) \doteq v_0, \text{ para } j \in J,$$

e

$$c_k \doteq v_0, \text{ para } k \in K,$$

obtém-se a validade das condições (I_2), (I_1') e (I_3'). Empregando ainda a equivalência sobre a fórmula

$$\neg v_0 \doteq v_1,$$

obtém-se, finalmente, a injetividade de τ.

■

Teorema 4.7.5 *As $\mathcal{L}$-estruturas $\mathfrak{A}$ de cardinalidade finita, e apenas elas, deixam-se caracterizar por um sistema de axiomas a menos de isomorfismos, ou seja, existe um conjunto $\Sigma \subset Sent_{\mathcal{L}}$, tal que, para toda $\mathcal{L}$-estrutura $\mathfrak{A}'$ vale:*

$$\mathfrak{A}' \models \Sigma \quad \textit{se e só se} \quad \mathfrak{A}' \simeq \mathfrak{A}$$

Prova. Inicialmente salientamos que se, a partir de uma $\mathcal{L}$-estrutura $\mathfrak{A}$, procuramos um sistema de axiomas Σ que satisfaça

$$\mathfrak{A}' \models \Sigma \quad \text{se e só se} \quad \mathfrak{A}' \simeq \mathfrak{A},$$

para toda $\mathcal{L}$-estrutura $\mathfrak{A}'$, então tomando $\mathfrak{A}' = \mathfrak{A}$ temos $\mathfrak{A} \simeq \mathfrak{A}$ e portanto deve ocorrer $\mathfrak{A} \models \Sigma$, ou seja,

$$\Sigma \subset Th_{\mathcal{L}}(\mathfrak{A}).$$

Assim, para encontrarmos um sistema de axiomas conveniente, obviamente deveremos buscá-lo dentro de $Th_{\mathcal{L}}(\mathfrak{A})$.

Supondo que isto acontece, temos que, se $\mathfrak{A}' \simeq \mathfrak{A}$ então, pelo Teorema 4.7.3, temos $\mathfrak{A}' \equiv \mathfrak{A}$, e portanto, como $\Sigma \subset Th_{\mathcal{L}}(\mathfrak{A})$, temos $\mathfrak{A}' \models \Sigma$.

Resta-nos assim provar a recíproca. Para tal, afirmamos inicialmente que para que exista um tal sistema de axiomas, $\mathfrak{A}$ tem que ter necessariamente cardinalidade finita. De fato, caso contrário, pelo Corolário 4.6.5, para esta estrutura infinita $\mathfrak{A}$ existe uma estrutura $\mathfrak{A}'$ elementarmente equivalente a ela com cardinalidade

$$\kappa > \mathsf{card}(|\mathfrak{A}|).$$

Assim, vale

$$\mathfrak{A}' \models Th_{\mathcal{L}}(\mathfrak{A}),$$

em particular

$$\mathfrak{A}' \models \Sigma,$$

mas não é verdade que $\mathfrak{A} \simeq \mathfrak{A}'$.

Fixemos n como sendo o número de elementos de $|\mathfrak{A}|$.

- No caso em que os conjuntos de índices I, J, K são finitos, afirmamos que podemos tomar Σ unitário. Mais precisamente, existe uma sentença $\alpha \in Th_{\mathcal{L}}(\mathfrak{A})$ tal que $\Sigma := \{\alpha\}$ serve, isto é, para toda $\mathcal{L}$-estrutura $\mathfrak{A}'$ vale:

$$\mathfrak{A}' \models \alpha \;\Rightarrow\; \mathfrak{A} \simeq \mathfrak{A}',$$

a saber, α é a conjunção de uma quantidade finita de $\mathcal{L}$-sentenças, as quais valem em $\mathfrak{A}$: como primeiro membro da conjunção, tomamos uma sentença $\alpha_{\leq n}$ que assegura que $|\mathfrak{A}'|$ possui no máximo tantos elementos quanto $|\mathfrak{A}|$, isto é, no máximo n elementos:

$$\alpha_{\leq n} := \exists\, v_1, ..., v_n \,\forall\, v_0\; (v_0 \doteq v_1 \vee ... \vee v_0 \doteq v_n).$$

Assim, se valer $\alpha_{\leq n}$ em $\mathfrak{A}'$, então evidentemente $|\mathfrak{A}'|$ tem no máximo n elementos. Sejam agora $a_1, ..., a_n$ os elementos de $|\mathfrak{A}|$. Para toda avaliação h em $\mathfrak{A}$ satisfazendo

$$h(v_i) = a_i \tag{92}$$

para $1 \leq i \leq n$ consideramos o conjunto Φ de todas as fórmulas, as quais valem por uma destas avaliações h em $\mathfrak{A}$ e que por outro lado são de um dos seguintes tipos:

$$x_0 \neq x_1$$

$$R_i(x_1, ..., x_{\lambda(i)}) \text{ com } i \in I$$

$$\neg R_i(x_1, ..., x_{\lambda(i)}) \text{ com } i \in I$$

$$f_j(x_1, ..., x_{\mu(j)}) \doteq x_0 \text{ com } j \in J$$

$$c_k \doteq x_0 \text{ com } k \in K$$

e $x_0, x_1, ... \in \{v_1, ..., v_n\}$. Convence-se com isto que Φ é um conjunto finito. Seja $\bigwedge \Phi$ a conjunção de todas as fórmulas de Φ. Afirmamos que a sentença procurada é

$$\alpha := (\alpha_{\leq n} \wedge \exists\, v_1, ..., v_n \bigwedge \Phi).$$

Se $\mathfrak{A}'$ é tal que α vale em $\mathfrak{A}'$, então, em primeiro lugar, $|\mathfrak{A}'|$ tem no máximo n elementos (pois $\mathfrak{A}' \models \alpha_{\leq n}$) e, em segundo lugar, existe uma avaliação h' em $\mathfrak{A}'$ com $\mathfrak{A}' \models \varphi[h']$ para toda $\varphi \in \Phi$. Obtemos assim uma aplicação

$$\tau : |\mathfrak{A}| \to |\mathfrak{A}'|,$$

dada por $\tau(a_i) = h'(v_i)$, para todo $1 \leq i \leq n$. tal que, para toda fórmula φ de um dos cinco tipos acima e para toda avaliação h que satisfaz (92), vale:

$$\mathfrak{A} \models \varphi[h] \;\Rightarrow\; \mathfrak{A}' \models \varphi[\tau \circ h].$$

A validade desta implicação tem como conseqüência precisamente a injetividade de τ (por causa das fórmulas do tipo $x_0 \neq x_1$ em Φ) e as condições (I_2), (I_1') e (I_3'). Assim, τ é um monomorfismo de $\mathfrak{A}$ em $\mathfrak{A}'$ e, como $\mathfrak{A}'$ tem no máximo n elementos, τ é até um isomorfismo.

- No caso em que os conjuntos de índices I, J e K são quaisquer, tomamos $\Sigma := Th_{\mathcal{L}}(\mathfrak{A})$. Supomos que $\mathfrak{A}'$ é um modelo de $Th_{\mathcal{L}}(\mathfrak{A})$. Por $\alpha_{\leq n} \in Th_{\mathcal{L}}(\mathfrak{A})$, temos que $|\mathfrak{A}'|$ tem no máximo n elementos.

Assim existe apenas um número finito de aplicações

$$\tau : |\mathfrak{A}| \to |\mathfrak{A}'|,$$

que vamos denotar por $\tau_1, ..., \tau_m$.Suponhamos que nenhuma destas aplicações é um isomorfismo. Se τ_ν não é isomorfismo, então τ_ν não é injetiva ou ou existe um índice $j \in J$ ou $i \in I$ ou $k \in K$ "ruim", isto é, tal que uma das condições $(I_1), (I_2)$ ou (I_3) não é satisfeita para τ_ν. Para cada τ_ν injetiva, para $1 \leq \nu \leq m$ fixamos um tal índice "ruim". Note que então estaremos fixando no máximo m índices, e com eles estaremos formando subconjuntos finitos I_1 de I, J_1 de J e K_1 de K. Estes subconjuntos definem uma sublinguagem $\mathcal{L}_1$ de $\mathcal{L}$. Sejam $\mathfrak{A}_1$ e $\mathfrak{A}'_1$ as restrições das $\mathcal{L}$-estruturas $\mathfrak{A}$ e $\mathfrak{A}'$ sobre a linguagem $\mathcal{L}_1$ (elas são obtidas simplesmente desconsiderando as interpretações de R_i para $i \in I \backslash I_1$, de f_j para $j \in J \backslash J_1$ e de c_k para $k \in K \backslash K_1$). Aplicando o caso particular acima provado para os subconjuntos finitos I_1, J_1 e K_1, concluímos que existe um isomorfismo

$$\tau : \mathfrak{A}_1 \leftrightarrow \mathfrak{A}'_1,$$

que é portanto uma função injetora. Como $\mathfrak{A}_1$ e $\mathfrak{A}'_1$ têm o mesmo domínio que $\mathfrak{A}$ e $\mathfrak{A}'$, respectivamente, τ deve coincidir com alguma das aplicações τ_ν e portanto tal τ_ν é injetora. Porém nenhuma τ_v pode ser isomorfismo de $\mathfrak{A}_1$ e $\mathfrak{A}'_1$, pois o "índice ruim" a ela associado pertence a $I_1 \cup J_1 \cup K_1$. Esta contradição mostra que de fato alguma das aplicações $\tau_1, ..., \tau_m$ deve ser um isomorfismo entre $\mathfrak{A}$ e $\mathfrak{A}'$.

■

Introduzimos agora uma notação sugestiva para

$$\mathfrak{A} \models \varphi[h],$$

a qual se faz útil pelo Lema 4.4.7, já que a validade de uma fórmula φ em $\mathfrak{A}$ depende apenas das avaliações das variáveis livres de φ.

Notação 4.7.6 *Se* $Fr(\varphi) \subset \{v_0, ..., v_n\}$ *e* $a_0, ..., a_n \in |\mathfrak{A}|$, *então escreveremos simplesmente*

$$\mathfrak{A} \models \varphi[a_0, ..., a_n]$$

para

$$\mathfrak{A} \models \varphi[h],$$

onde h *é alguma avaliação em* $\mathfrak{A}$ *com* $a_\nu = h(v_\nu)$ *para* $0 \leq \nu \leq n$. *Para*

$$\mathfrak{A} \models \varphi[h(x, a)]$$

escreveremos também

$$\mathfrak{A} \models \varphi[a_0, ..., a_n, (x, a)].$$

Salientamos que, utilizando esta forma de escrita, a afirmação contida no enunciado do Teorema 4.7.3 pode ser expressa da seguinte maneira: Para cada $\mathcal{L}$*-fórmula* φ *com* $Fr(\varphi) \subset \{v_0, ..., v_n\}$ *e todo* $a_0, ..., a_n \in |\mathfrak{A}|$ *vale*

$$\mathfrak{A} \models \varphi[a_0, ..., a_n] \Leftrightarrow \mathfrak{A}' \models \varphi[\tau(a_0), ..., \tau(a_n)].$$

4.8 Subestruturas

Nesta seção apresentamos a construção, devida a Löwenhein e Skolem, de subestrutura elementar de uma $\mathcal{L}$-estrutura dada, e que, em particular, é elementarmente equivalente à primeira.

Começamos por estas definições:

Definição 4.8.1 *Uma* $\mathcal{L}$*-estrutura* $\mathfrak{B}$ *é dita uma* <u>subestrutura</u> *de uma* $\mathcal{L}$*-estrutura* $\mathfrak{A}$ *(ou* $\mathfrak{A}$ *é uma* <u>estrutura estendida</u> *de* $\mathfrak{B}$*) se*

$$|\mathfrak{B}| \subset |\mathfrak{A}|$$

e a função identidade

$$id : |\mathfrak{B}| \to |\mathfrak{A}|$$

é um monomorfismo entre as estruturas $\mathfrak{A}$ *e* $\mathfrak{B}$. *Isto significa que, para*

$a_1, ... \in |\mathfrak{B}|$, $i \in I$, $j \in J$ e $k \in K$,

$$R_i^{\mathfrak{B}}(a_1, ...) \quad \textit{se e só se} \quad R_i^{\mathfrak{A}}(a_1, ...)$$

$$f_j^{\mathfrak{B}}(a_1, ...) = f_j^{\mathfrak{A}}(a_1, ...),$$

$$c_k^{\mathfrak{B}} = c_k^{\mathfrak{A}}.$$

Notação 4.8.2 *Para significar que $\mathfrak{B}$ é subestrutura de $\mathfrak{A}$ escreveremos*

$$\mathfrak{B} \subset \mathfrak{A}.$$

Salientamos que, se $\mathfrak{B}$ é uma subestrutura de $\mathfrak{A}$, então o subconjunto $|\mathfrak{B}| = B$ de $|\mathfrak{A}|$ possui as seguintes propriedades:

$$\left.\begin{array}{l} (i)\ B \text{ é fechado sob as funções } f_j^{\mathfrak{A}}, \text{ ou seja, para todo} \\ a_1, ..., a_{\mu(j)} \in B \text{ vale que } f_j^{\mathfrak{A}}(a_1, ..., a_{\mu(j)}) \in B, \\ (ii)\ \text{as interpretações das constantes } c_k^{\mathfrak{A}} \text{ caem em } B: \\ c_k^{\mathfrak{A}} \in B, \end{array}\right\} \quad (93)$$

Reciprocamente:

Definição 4.8.3 *Se um subconjunto B de $|\mathfrak{A}|$ satisfaz as propriedades (i) e (ii) acima, então a $\mathcal{L}$-estrutura*

$$\mathfrak{B} := \left\langle B; (R_i^{\mathfrak{A}}|_B)_{i\in I}; (f_j^{\mathfrak{A}}|_B)_{j\in J}; (c_k^{\mathfrak{A}})_{k\in K} \right\rangle,$$

onde $R_i^{\mathfrak{A}}|_B$ e $f_j^{\mathfrak{A}}|_B$ são as restições das relações $R_i^{\mathfrak{A}}$ e funções $f_j^{\mathfrak{A}}$ ao subconjunto B, é evidentemente uma subestrutura de $\mathfrak{A}$, chamada estrutura definida por B.

Definição 4.8.4 *Uma subestrutura $\mathfrak{B}$ de $\mathfrak{A}$ chama-se uma subestrutura elementar de $\mathfrak{A}$ se, para toda $\mathcal{L}$-fórmula φ e toda avaliação h em $\mathfrak{B}$,*

$$\mathfrak{B} \models \varphi[h] \quad \textit{se e só se} \quad \mathfrak{A} \models \varphi[h].$$

Notação 4.8.5 *Se $\mathfrak{B}$ é uma subestrutura elementar de $\mathfrak{A}$, então escreve-*

remos

$$\mathfrak{B} \prec \mathfrak{A}.$$

Trivialmente segue que

$$\mathfrak{B} \prec \mathfrak{A} \quad \text{implica} \quad \mathfrak{B} \equiv \mathfrak{A}.$$

Porém não vale a recíproca, assim como no seguinte exemplo:

Exemplo 4.8.6 *Na linguagem de grupos totalmente ordenados, consideramos as estruturas*

$$\langle \mathbb{N}^*; \leq \rangle \subset \langle \mathbb{N}; \leq \rangle,$$

onde $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ *e* $\leq$ *é a relação usual de menor ou igual. Como*

$$n \mapsto n - 1$$

é uma bijeção de $\mathbb{N}^*$ *em* $\mathbb{N}$*, podemos afirmar que*

$$\langle \mathbb{N}^*; \leq \rangle \simeq \langle \mathbb{N}; \leq \rangle.$$

Assim, pelo Teorema 4.7.3,

$$\langle \mathbb{N}^*; \leq \rangle \equiv \langle \mathbb{N}; \leq \rangle.$$

No entanto, $\langle \mathbb{N}^*; \leq \rangle$ *não é subestrutura elementar de* $\langle \mathbb{N}; \leq \rangle$*, pois a fórmula*

$$\forall v_1 \; v_0 \leq v_1$$

por uma avaliação h *em* $\langle \mathbb{N}^*; \leq \rangle$*, com* $h(v_0) = 1$*, vale em* $\langle \mathbb{N}^*; \leq \rangle$*, mas não vale em* $\langle \mathbb{N}; \leq \rangle$*.*

Contudo, podemos verificar, pela definição dada, que na linguagem $\mathcal{L}$ *que possui apenas um símbolo, o relacional* $<$*, cuja interpretação dada em* $\mathbb{R}$ *e* $\mathbb{Q}$ *é a mesma da relação usual "menor", vale*

$$\langle \mathbb{Q}; < \rangle \prec \langle \mathbb{R}; < \rangle,$$

Basta observar que aqui apenas as variáveis são termos, e as fórmulas atômicas são de um de dois tipos:

$$x \doteq y \quad ou \quad x < y.$$

Claramente estas fórmulas são válidas por uma avaliação h de $\langle \mathbb{Q}; < \rangle$ em $\langle \mathbb{Q}; < \rangle$ se e somente se são válidas por esta avaliação em $\langle \mathbb{R}; < \rangle$. Como a validade de uma fórmula mais geral (com operadores lógicos) só depende dos valores lógicos atribuídos às fórmulas atômicas, é verdadeira a relação acima.

Lema 4.8.7 *Seja $\mathfrak{B}$ uma subestrutura de $\mathfrak{A}$. Se, para cada quantidade finita de elementos $a_1, ...a_n \in |\mathfrak{B}|$ e cada $a \in |\mathfrak{A}|$ existe um automorfismo τ de $\mathfrak{A}$ com $\tau(a_i) = a_i$ para $1 \leq i \leq n$ e $\tau(a) \in |\mathfrak{B}|$, então $\mathfrak{B}$ é uma subestrutura elementar de $\mathfrak{A}$.*

Prova. Mostramos por indução sobre a construção das fórmulas que, para toda fórmula φ e toda avaliação h em $\mathfrak{B}$,

$$\mathfrak{B} \models \varphi[h] \quad \text{se e só se} \quad \mathfrak{A} \models \varphi[h].$$

Esta prova é completamente análoga à prova do Teorema 4.7.3 (quando colocamos lá $\tau = id$) até o momento em que passamos a tratar, no passo de indução, o caso em que φ é da forma $\forall x\ \psi$ (pois lá foi usada a sobrejetividade de τ, o que aqui não temos assegurada). Neste caso, decompomos a prova da equivalência acima em duas partes:

Caso 1 : $\mathfrak{A} \models \forall x\ \psi[h]$. Neste caso, temos

$$\mathfrak{A} \models \psi[h(x, a)],$$

para todo $a \in |\mathfrak{A}|$. Como $h(x, a)$ é uma avaliação em $\mathfrak{B}$ para todo $a \in |\mathfrak{B}|$, temos, pela hipótese de indução,

$$\mathfrak{B} \models \psi[h(x, a)].$$

Pela definição de validade temos, finalmente,

$$\mathfrak{B} \models \forall x\ \psi[h].$$

Caso 2: $\mathfrak{A} \not\models \forall x\ \psi[h]$: Neste caso, existe um $a \in |\mathfrak{A}|$ tal que

$$\mathfrak{A} \not\models \psi[h(x, a)].$$

Sejam $x_1, ..., x_n$ todas as variáveis livres de $\forall x\ \psi$. Escolhemos um automorfismo τ de $\mathfrak{A}$ que satisfaz

$$\tau(h(x_i)) = h(x_i), \tag{94}$$

para $1 \leq i \leq n$ e

$$\tau(h(x, a)(x)) = \tau(a) \in |\mathfrak{B}|,$$

que existe, por hipótese.

Empregando o Teorema 4.7.3 sobre o automorfismo τ de $\mathfrak{A}$, obtemos

$$\mathfrak{A} \not\models \psi[\tau \circ h(x, a)].$$

Note que, então, por (94), $\tau \circ h$ e h coincidem nas variáveis livres de $\forall x\ \psi$ e portanto

$$\tau \circ h(x, a) = (\tau \circ h)(x, \tau(a))$$

e

$$h(x, \tau(a))$$

coincidem em todas as variáveis livres de ψ. Com isto e com o Lema 4.4.7 obtemos

$$\mathfrak{A} \not\models \psi[h(x, \tau(a))].$$

A hipótese de indução nos permite afirmar então

$$\mathfrak{B} \not\models \psi[h(x, \tau(a))],$$

o que finalmente nos leva a

$$\mathfrak{B} \not\models \forall x \ \psi[h].$$

■

Chegamos agora a um método para construir subestruturas elementares devido a Löwenheim e Skolem.

Teorema 4.8.8 (Lowenheim-Skolem) *Sejam $\mathfrak{A}$ uma $\mathcal{L}$-estrutura de cardinalidade infinita e C um subconjunto de $|\mathfrak{A}|$. Então existe uma subestrutura elementar $\mathfrak{B}$ de $\mathfrak{A}$ com $C \subset B = |\mathfrak{B}|$ é tal que*

$$\mathsf{card}(C) \leq \mathsf{card}(B) \leq \max(\kappa_{\mathcal{L}}, \ \mathsf{card}(C)).$$

Em particular, $\kappa_{\mathcal{L}} \leq \mathsf{card}(C)$, então segue que $\mathsf{card}(B) = \mathsf{card}(C)$.

Prova. Denotemos $|\mathfrak{A}| = A$. Vamos construir o domínio B como uma união

$$B = \bigcup_{m \in \mathbb{N}} B_m,$$

onde os B_m são definidos recursivamente a partir de

$$B_0 = C.$$

Mais precisamente, para todo $m \geq 0$,

$$B_{m+1} = B_m \ \cup \bigcup_{\varphi} g_{\varphi}(B_m^{(n_\varphi+1)}) \tag{95}$$

sendo a união acima considerada sobre todas as fórmulas existenciais φ com parâmetros em $\mathfrak{A}$. Como de hábito,

$$B_m^{(n_\varphi+1)}$$

denota o produto cartesiano de $(n_\varphi + 1)$ cópias de B_m. No caso de

$$n_\varphi = -1$$

consideramos $B_m^{(n_\varphi+1)} = B_m^0 = \emptyset$.

Passamos a definir o número n_φ e as funções g_φ.

Para cada fórmula existencial φ do tipo $\exists x\ \psi$, denotamos por n_φ o mais alto índice de uma variável livre de φ (relembramos que a primeira variável é denotada por v_0) sendo que, se ψ é apenas uma sentença, então definimos $n_\varphi = -1$.

A seguir, definimos a $(n_\varphi + 1)$-ária função g_φ sobre $A = |\mathfrak{A}|$ da seguinte maneira: fixado um elemento $d_0 \in A$,

- Se $n_\varphi \geq 0$: dados $a_0, ..., a_{n_\varphi} \in A$ e h uma avaliação qualquer que satisfaça

$$h(v_s) = a_s,$$

para $0 \leq s \leq n_\varphi$, então

$$g_\varphi(a_0, ..., a_{n_\varphi}) = \begin{cases} a \in A, \text{ caso } \mathfrak{A} \models \exists x\ \psi[h], \text{ mais precisamente,} \\ \mathfrak{A} \models \psi[h(x, a)], \\ \\ d_0, \text{ caso contrário,} \end{cases}$$

Salientamos que g_φ não é determinada univocamente, o que não traz prejuízos à idéia que queremos aqui utilizar.

- Se $n_\varphi = -1$ e $\mathfrak{A} \models \exists x\ \psi$ então definimos $g_\varphi(\emptyset)$ como sendo o elemento $a \in A$ que satisfaz

$$\mathfrak{A} \models \psi[h(x, a)];$$

- Se $n_\varphi = -1$ e $\mathfrak{A} \not\models \exists x\ \psi$ então definimos $g_\varphi(\emptyset)$ como sendo d_0

Afirmamos que o conjunto B acima satisfaz as condições (i) e (ii) de (93), e portanto define uma subestrutura de $\mathfrak{A}$. De fato:

- Para $k \in K$ escolhemos a sentença existencial

$$\varphi := \exists\ v_0\ (v_0 \doteq c_k).$$

Para cada avaliação h, existe um $a \in A$ tal que

$$\mathfrak{A} \models (v_0 \doteq c_k)[h(v_0, a)],$$

a saber,

$$a = c_k^{\mathfrak{A}}.$$

Assim, $g_\varphi(\emptyset)$ é igual a algum conjunto unitário $\{a\}$.

Como existe apenas um tal a, também podemos escrever $g_\varphi = c_k^{\mathfrak{A}}$. Com isto, temos

$$a = c_k^{\mathfrak{A}} \in g_\varphi(\emptyset) \overset{(95)}{\subset} B_1 \subset B.$$

- Para cada $j \in J$ e para fixados $a_0, a_1, ..., a_{\mu(j)-1} \in B$ (digamos, $a_0, a_1, ..., a_{n_\varphi} = a_{\mu(j)-1} \in B_m$) para mostrarmos que $a := f_j^{\mathfrak{A}}(a_0, ..., a_{\mu(j)-1}) \in B$ consideramos a fórmula existencial

$$\varphi := \exists v_{\mu(j)} \ (v_{\mu(j)} \doteq f_j(v_0, ..., v_{\mu(j)-1})),$$

que obviamente vale em $\mathfrak{A}$.

Neste caso, $n_\varphi = \mu(j)-1$, e portanto a aridade da correspondente função g_φ é $n_\varphi + 1 = \mu(j)$. Considerando a a avaliação h dada por $h(v_s) = a_s$ para $0 \leq s \leq (\mu(j) - 1)$, temos que ,

$$\mathfrak{A} \models \exists v_{\mu(j)} \ \ v_{\mu(j)} \doteq f_j(v_0, ..., v_{\mu(j)-1})[h],$$

a saber,

$$\mathfrak{A} \models v_{\mu(j)} \doteq f_j(v_0, ..., v_{\mu(j)-1})[h(v_{\mu(j)}, a)].$$

Pela definição de g_φ,

$$a_{\mu(j)} = g_\varphi(a_0, ..., a_{n_\varphi}) \in B_{m+1} \subset B.$$

Salientamos que, como φ envolve exclusivamente um símbolo funcional e uma igualdade, temos $a_{\mu(j)} = a$ e portanto $a \in B_{m+1} \subset B$.

Temos assim, por (93), garantida a existência de uma subestrutura de $\mathfrak{A}$ definida por B, e que vamos denotar por $\mathfrak{B}$.

Afirmamos que $\mathfrak{B}$ é até uma subestrutura elementar de $\mathfrak{A}$. De forma análoga à prova do Lema 4.8.7, fazemos uma prova por indução sobre a construção de uma fórmula. E, para tal, basta novamente provarmos que, no caso de uma fórmula do tipo $\forall x\ \psi$, sua não validade (para uma avaliação h em $\mathfrak{B}$) transfere-se de $\mathfrak{A}$ para $\mathfrak{B}$. Suponhamos, assim, que

$$\mathfrak{A} \not\models \forall x\ \psi[h].$$

Então

$$\mathfrak{A} \models \varphi[h]$$

para a fórmula existencial

$$\varphi = \exists x\ \neg\psi.$$

Seja m tal que

$$h(v_0), ..., h(v_{n_\varphi}) \in B_m \subset B.$$

Então, por construção, por um lado

$$a = g_\varphi(h(v_0), ..., h(v_{n_\varphi})) \in B_{m+1}$$

e portanto a é um elemento de B tal que

$$\mathfrak{A} \models \neg\psi[h(x, a)].$$

Agora, como $a \in B$, temos que $h(x, a)$ é também uma avaliação em $\mathfrak{B}$, e portanto pela hipótese de indução, segue que

$$\mathfrak{B} \models \neg\psi[h(x, a)].$$

Em particular,

$$\mathfrak{B} \models \exists x\ \neg\psi[h].$$

Com isto, temos a prova de que

$$\mathfrak{B} \not\models \forall x\ \psi[h].$$

Resta-nos estimar a cardinalidade de $\mathfrak{B}$. Basta mostrar que, para cada m,

$$\mathsf{card}(B_m) \leq \max(\kappa_{\mathcal{L}}, \mathsf{card}(C)) =: \kappa.$$

Para $B_0 = C$ isto é claro. Suponha que a estimativa acima vale para B_m. De (95), segue que

$$\begin{aligned}\mathsf{card}(B_{m+1}) &\leq \max(\mathsf{card}(B_m), \mathsf{card}(\bigcup_{\varphi} g_\varphi(B_m^{(n_\varphi+1)})) \\ &\leq \max(\kappa, \mathsf{card}(Fml_{\mathcal{L}})) = \kappa,\end{aligned}$$

pois cada termo $g_\varphi\ (B_m^{(n_\varphi+1)})$ da união, bem como B_m, tem cardinalidade $\leq \kappa$ e a união é indexada com um subconjunto de $Fml_{\mathcal{L}}$, e vale $\mathsf{card}(Fml_{\mathcal{L}}) = \kappa_{\mathcal{L}}$ pela equação (84).

■

Observação 4.8.9 *A construção feita na demonstração acima pode ser comparada com a construção do fecho algébrico de um corpo F dentro de uma extensão de corpos $L|F$ com L algebricamente fechado: no caso de corpos a extensão é obtida acrescentando-se as raízes de polinômios com coeficientes em F que pertencem a L. Note que estamos tratando de sentenças existenciais com parâmetros em F.*

Corolário 4.8.10 *Se $\mathcal{L}$ é uma linguagem enumerável, isto é, $\kappa_{\mathcal{L}} = \aleph_0$, então cada $\mathcal{L}$-estrutura $\mathfrak{A}$ de cardinalidade infinita possui uma subestrutura elementar $\mathfrak{B}$ enumerável.*

Prova. Escolhemos, no Teorema 4.8.8,

$$C = B_0 = \emptyset.$$

Daí segue que

$$\mathsf{card}(B) \leq \aleph_0.$$

Porém B não pode ser finito, pois senão haveria uma sentença da forma $\alpha_{\leq n}$ (considerada na prova do Teorema 4.7.5) que vale em $\mathfrak{B}$ e naturalmente não vale em $\mathfrak{A}$. Assim,

$$\mathsf{card}(B) = \aleph_0,$$

ou seja, $\mathfrak{B}$ é enumerável.

■

Encerramos esta seção generalizando a definição de subestrutura elementar:

Definição 4.8.11 *Um monomorfismo $\tau : \mathfrak{A} \to \mathfrak{A}'$ de $\mathcal{L}$-estruturas chama-se uma imersão elementar, se para toda fórmula φ e cada avaliação h em $\mathfrak{A}$ vale:*

$$\mathfrak{A} \models \varphi[h] \quad \textit{se e só se} \quad \mathfrak{A}' \models \varphi[\tau \circ h].$$

Empregando a definição acima sobre as $\mathcal{L}$-sentenças obtemos em particular $\mathfrak{A} \equiv \mathfrak{A}'$.

4.9 Extensões elementares e Cadeias

Na seção anterior apresentamos uma maneira de construir, a partir de uma $\mathcal{L}$-estrutura dada, uma subestrutura elementar. Aqui vamos nos preocupar em construir uma extensão elementar, e o fazemos de duas maneiras distintas.

Iniciamos complementando a Definição 4.8.4:

Definição 4.9.1 *Dadas duas $\mathcal{L}$-estruturas $\mathfrak{A}$ e $\mathfrak{B}$, dizemos que $\mathfrak{B}$ é uma extensão elementar de $\mathfrak{A}$, caso $\mathfrak{A}$ seja uma subestrutura elementar de $\mathfrak{B}$.*

A primeira maneira de obter uma extensão elementar é ampliando a linguagem por constantes, o que passamos a tratar agora.

Notação 4.9.2 *Relembramos (veja Definição 4.1.1) que uma extensão por constantes de uma linguagem $\mathcal{L} = (\lambda, \mu, K)$ é uma extensão da forma*

$\mathcal{L}' = (\lambda', \mu', K')$, *onde* $\lambda' = \lambda$, $\mu' = \mu$ *e* $K' = K \cup \underline{K}$ *e* $K \cap \underline{K} = \emptyset$. *O conjunto* $\underline{K}$ *atua assim como conjunto de índices para as novas constantes. Uma* $\mathcal{L}'$*-estrutura* $\mathfrak{A}'$ *é portanto uma* $\mathcal{L}$*-estrutura* $\mathfrak{A}$ *juntamente com uma interpretação para as novas constantes, interpretação esta que vamos esvrever na forma*

$$\sigma : \underline{K} \to |\mathfrak{A}|$$

onde $\sigma(k) = c_k^{\mathfrak{A}'}$ *para* $k \in \underline{K}$. *Com uma tal notação, denotamos esta* $\mathcal{L}'$*-estrutura* $\mathfrak{A}'$ *por*

$$\mathfrak{A}' = (\mathfrak{A}, \sigma)$$

assim, $\mathfrak{A}$ *é a restrição de* $\mathfrak{A}'$ *sobre* $\mathcal{L}$. .

Lema 4.9.3 *Seja* $\mathcal{L}' = (\lambda', \mu', K')$ *uma ampliação por constantes da linguagem* $\mathcal{L} = (\lambda, \mu, K)$, *onde* $K' = K \cup \underline{K}$ *e* $K \cap \underline{K} = \emptyset$. *Sejam* $\mathfrak{A}' = (\mathfrak{A}, \sigma)$ *uma* $\mathcal{L}'$*-estrutura e* φ *uma* $\mathcal{L}$*-fórmula com* $Fr(\varphi) \subset \{v_0, ..., v_n\}$. *Então vale, para todos* $k_0, ..., k_n \in \underline{K}$ *e toda avaliação* h *em* $\mathfrak{A}$ *satisfazendo* $h(v_s) = \sigma(k_s) = c_{k_s}^{\mathfrak{A}'}$ *para* $0 \leq s \leq n$*:*

$$\mathfrak{A} \models \varphi[h] \quad \textit{se e só se} \quad (\mathfrak{A}, \sigma) \models \varphi(v_0/c_{k_0}, ..., v_n/c_{k_n}).$$

Prova. Salientamos inicialmente que $\mathfrak{A}' \models \varphi(v_0/c_{k_0}, ..., v_n/c_{k_n})$ faz sentido, pois sendo φ uma $\mathcal{L}$-fórmula, $\varphi(v_0/c_{k_0}, ..., v_n/c_{k_n})$ é uma $\mathcal{L}'$-fórmula.

Empregamos aqui iteradas vezes o Lema 4.4.11: para a primeira variável v_0, obtemos, para qualquer avaliação h que satisfaz $h(v_0) = c_{k_0}^{\mathfrak{A}'}[h] = c_{k_0}^{\mathfrak{A}'} = \sigma(k_0)$,

$$\mathfrak{A} \models \varphi[h] \quad \text{se e só se} \quad \mathfrak{A}' \models \varphi[h(v_0, c_{k_0})] \quad \text{se e só se} \quad \mathfrak{A}' \models \varphi(v_0/c_{k_0})[h].$$

Repetindo o processo para as demais variáveis, obtemos finalmente

$$\mathfrak{A} \models \varphi[h] \quad \text{se e só se} \quad \mathfrak{A}' \models \varphi(v_0/c_{k_0}, ..., v_n/c_{k_n})[h].$$

Isto no entanto prova a afirmação do lema, pois como foram esgotadas

todas as variáveis livres envolvidas em φ, temos

$$\mathfrak{A}' \models \varphi(v_0/c_{k_0}, ..., v_n/c_{k_n})[h] \quad \text{se e só se} \quad \mathfrak{A}' \models \varphi(v_0/c_{k_0}, ..., v_n/c_{k_n}).$$

■

Um caso particular de extensão por constantes $\mathcal{L}'$ de $\mathcal{L}$ é quando o conjunto $\underline{K}$ tem alguma relação com a $\mathcal{L}$-estrutura $\mathfrak{A}$: seja A' um subconjunto de $|\mathfrak{A}|$. Suponhamos, sem perda de generalidade, que $K \cap |\mathfrak{A}| = \emptyset$, e definamos então $\underline{K} = A'$. Neste caso, escreveremos

$$\underline{a} := c_a,$$

para todo $a \in \underline{K}$. Um exemplo de interpretação para as novas constantes $\underline{a}$ em $\mathfrak{A}$ é a interpretação canônica, ou seja , usamos $\underline{a}$ para denotar a constante associada ao elemento $a \in A'$. A $\mathcal{L}'$-estrutura canônica obtida de $\mathfrak{A}$ é neste caso $(\mathfrak{A}, \sigma) = (\mathfrak{A}, id_{A'})$, que vamos denotar por

$$(\mathfrak{A}, A') := (\mathfrak{A}, id_{A'}).$$

Lembramos que neste caso podemos escrever

$$\mathcal{L}' = \mathcal{L}(A') = \mathcal{L}_{A'}$$

Notação 4.9.4 *Se tivermos $A' = |\mathfrak{A}|$, então cada elemento $a \in |\mathfrak{A}|$ possui pelo menos um símbolo para ele, a saber $\underline{a}$, na linguagem $\mathcal{L}(|\mathfrak{A}|)$. Neste caso, escreveremos resumidamente $\mathcal{L}(\mathfrak{A})$ para $\mathcal{L}(|\mathfrak{A}|)$.*

Com a notação acima, a conclusão do Lema 4.9.3 escreve-se agora na forma

$$\mathfrak{A} \models \varphi[a_0, ..., a_n] \quad \text{se e só se} \quad (\mathfrak{A}, |\mathfrak{A}|) \models \varphi(v_0/\underline{a_0}, ..., v_n/\underline{a_n}).$$

Definição 4.9.5 *Se $\mathfrak{A}$ é uma $\mathcal{L}$-estrutura, então definimos o Diagrama de $\mathfrak{A}$ como sendo o conjunto $D(\mathfrak{A})$ formado por todas as $\mathcal{L}(\mathfrak{A})$-sentenças atômicas*

ou negações delas que valem em $(\mathfrak{A}, |\mathfrak{A}|)$*:*

$$D(\mathfrak{A}) = \{\varphi \mid \varphi \text{ é } \mathcal{L}(\mathfrak{A})\text{-sentença atômica e } \mathfrak{A} \models \varphi\} \cup \{\neg\varphi \mid \varphi \text{ é } \mathcal{L}(\mathfrak{A})\text{-sentença atômica e } \mathfrak{A} \models \neg\varphi\}$$

Aqui por sentença atômica estamos significando uma fórmula atômica que é até uma sentença.

O diagrama de $\mathfrak{A}$ é assim um subconjunto da Teoria de $(\mathfrak{A}, |\mathfrak{A}|)$, ou seja, do conjunto $Th_{\mathcal{L}(\mathfrak{A})}(\mathfrak{A}, |\mathfrak{A}|)$ de todas as $\mathcal{L}(\mathfrak{A})$-sentenças que valem em $(\mathfrak{A}, |\mathfrak{A}|)$.

Lema 4.9.6 (Lema do Diagrama) *Sejam* $\mathfrak{A}$ *uma* $\mathcal{L}$*-estrutura e* $(\mathfrak{B}, \sigma)$ *uma* $\mathcal{L}(\mathfrak{A})$*-estrutura.*

i) Se $(\mathfrak{B}, \sigma)$ *é um modelo de* $D(\mathfrak{A})$*, então* σ *é uma imersão de* $\mathfrak{A}$ *em* $\mathfrak{B}$*. Em particular, as* $\mathcal{L}(\mathfrak{A})$*-estruturas que são modelos de* $D(\mathfrak{A})$ *contêm uma cópia de* $\mathfrak{A}$*.*

ii) Se $(\mathfrak{B}, \sigma)$ *é modelo de* $Th_{\mathcal{L}(\mathfrak{A})}((\mathfrak{A}, |\mathfrak{A}|))$ *então* σ *é uma imersão elementar de* $\mathfrak{A}$ *em* $\mathfrak{B}$*.*

Prova. *i)* Pela definição de imersão, devemos mostrar que a aplicação

$$\sigma : |\mathfrak{A}| \to |\mathfrak{B}|$$

satisfaz as condições (I_1'), (I_2) e (I_3') da Definição 4.7.1 e que é injetiva.

Inicialmente provemos a injetividade de σ: dados $a_1, a_2 \in |\mathfrak{A}|$ distintos, temos que a sentença $(\underline{a_1} \neq \underline{a_2})$ (que não é atômica mas é a negação de uma) pertence ao diagrama $D(\mathfrak{A})$. Como $(\mathfrak{B}, \sigma)$ é também um modelo de $D(\mathfrak{A})$, temos

$$(\mathfrak{B}, \sigma) \models (\underline{a_1} \neq \underline{a_2}).$$

Mas a interpretação $\underline{a_i}$ em $(\mathfrak{B}, \sigma)$ é precisamente $\sigma(a_i)$; daí segue

$$\sigma(a_1) \neq \sigma(a_2).$$

A prova tanto de (I_1') como de (I_3') é feita de forma análoga, considerando

as respectivas sentenças:

$$f_j(\underline{a_1}, ..., \underline{a_{\mu(j)}}) \doteq \underline{d} \quad e \quad c_k \doteq \underline{d}.$$

Para provar (I_2), observamos que

$$R_i(\underline{a_1}, ..., \underline{a_{\lambda(i)}}) \in D(\mathfrak{A})$$

caso $R_i^{\mathfrak{A}}(a_1, ..., a_{\lambda(i)})$. Analogamente,

$$\neg R_i(\underline{a_1}, ..., \underline{a_{\lambda(i)}}) \in D(\mathfrak{A})$$

caso $R_i^{\mathfrak{A}}(a_1, ..., a_{\lambda(i)})$ não vale em $(\mathfrak{A}, |\mathfrak{A}|)$. Mas como $(\mathfrak{B}, \sigma)$ é um modelo de $D(\mathfrak{A})$,

$$\begin{aligned} R_i^{\mathfrak{A}}(a_1, ..., a_{\lambda(i)}) &\Leftrightarrow R_i(\underline{a_1}, ..., \underline{a_{\lambda(i)}}) \in D(\mathfrak{A}) \\ &\Rightarrow (\mathfrak{B}, \sigma) \models R_i(\underline{a_1}, ..., \underline{a_{\lambda(i)}}) \\ &\Leftrightarrow R_i^{\mathfrak{B}}(\sigma(a_1), ..., \sigma(a_{\lambda(i)}). \end{aligned}$$

Reciprocamente,

$$\begin{aligned} \text{não vale } R_i^{\mathfrak{A}}(a_1, ..., a_{\lambda(i)}) &\Leftrightarrow \neg R_i(\underline{a_1}, ..., \underline{a_{\lambda(i)}}) \in D(\mathfrak{A}) \\ &\Leftrightarrow (\mathfrak{B}, \sigma) \models \neg R_i(\underline{a_1}, ..., \underline{a_{\lambda(i)}}) \\ &\Leftrightarrow \text{não vale } R_i^{\mathfrak{B}}(\sigma(a_1), ..., \sigma(a_{\lambda(i)}). \end{aligned}$$

Provamos assim, que

$$R_i^{\mathfrak{A}}(a_1, ..., a_{\lambda(i)}) \text{ se e só se } R_i^{\mathfrak{B}}(\sigma(a_1), ..., \sigma(a_{\lambda(i)})),$$

o que completa a prova de *(i)*.

ii) Se $(\mathfrak{B}, \sigma)$ é um modelo de $Th(\mathfrak{A}, |\mathfrak{A}|)$ então, em particular, o é de $D(\mathfrak{A})$ também, já que

$$D(\mathfrak{A}) \subset Th(\mathfrak{A}, |\mathfrak{A}|).$$

Assim, por *(i)*, σ é novamente uma imersão. Afirmamos que neste caso σ

é até uma imersão elementar de $\mathfrak{A}$ em $\mathfrak{B}$, ou seja, para toda $\mathcal{L}$-fórmula φ com $Fr(\varphi) \subset \{v_0, ..., v_n\}$ e toda avaliação h em $\mathfrak{A}$, tem-se

$$\mathfrak{A} \models \varphi[h] \quad \text{se e só se} \quad \mathfrak{B} \models \varphi[\sigma \circ h].$$

Salientamos que basta provar

$$\mathfrak{A} \models \varphi[h] \quad \text{implica} \quad \mathfrak{B} \models \varphi[\sigma \circ h],$$

pois daí, utilizando o mesmo raciocínio para $\neg\varphi$, obtemos a implicação recíproca provada por contraposição:

$$\begin{aligned} &\mathfrak{A} \not\models \varphi[h] \Rightarrow \\ &\mathfrak{A} \models \neg\varphi[h] \Rightarrow \\ &\mathfrak{B} \models \neg\varphi[\sigma \circ h] \Rightarrow \\ &\mathfrak{B} \not\models \varphi[\sigma \circ h]. \end{aligned}$$

Fixamos então $a_s = h(v_s)$ para $0 \leq s \leq n$. Pelo Lema 4.9.3 temos

$$\mathfrak{A} \models \varphi[h] \quad \text{implica} \quad (\mathfrak{A}, |\mathfrak{A}|) \models \varphi(v_0/\underline{a_0}, ..., v_n/\underline{a_n}).$$

Assim, a sentença $\varphi(v_0/\underline{a_0}, ..., v_n/\underline{a_n})$ é um elemento de $Th(\mathfrak{A}, |\mathfrak{A}|)$, e com isto vale também em $(\mathfrak{B}, \sigma)$, que é por hipótese um modelo para esta teoria:

$$(\mathfrak{B}, \sigma) \models \varphi(v_0/\underline{a_0}, ..., v_n/\underline{a_n}).$$

Usando agora o Lema 4.9.3 sobre a avaliação $\sigma \circ h$ em $\mathfrak{B}$, e levando em conta que

$$(\sigma \circ h)(v_s) = \sigma(a_s),$$

obtemos finalmente

$$\mathfrak{B} \models \varphi[\sigma \circ h].$$

■

Observe que se $\mathfrak{A}$ é uma $\mathcal{L}$-estrutura de cardinalidade infinita, então podemos empregar o Teorema 4.6.3 sobre o conjunto de $\mathcal{L}(\mathfrak{A})$-sentenças

$\Sigma = Th(\mathfrak{A}, |\mathfrak{A}|)$ e obter um modelo $(\mathfrak{B}, \sigma)$ de Σ com cardinalidade κ, onde

$$\kappa \geq \kappa_{\mathcal{L}(\mathfrak{A})} = \max(\kappa_{\mathcal{L}}, card(|\mathfrak{A}|)).$$

Pelo Lema do Diagrama, σ é uma imersão elementar de $\mathfrak{A}$ em $\mathfrak{B}$. Identificando $\mathfrak{A}$ com sua imagem por σ em $\mathfrak{B}$, temos provado o

Teorema 4.9.7 *Seja $\mathfrak{A}$ uma $\mathcal{L}$-estrutura de cardinalidade infinita. Para todo número cardinal*

$$\kappa \geq \max(\kappa_{\mathcal{L}}, card(|\mathfrak{A}|))$$

existe uma extensão elementar $\mathfrak{B}$ de $\mathfrak{A}$ com cardinalidade κ.

Os próximos dois resultados são conseqüências do Lema do Diagrama importantes na prática. A primeira delas é conseqüência da segunda parte do lema:

Corolário 4.9.8 *Sejam $\mathfrak{A}$ e $\mathfrak{B}$ duas $\mathcal{L}$-estruturas. Uma imersão*

$$\tau : \mathfrak{A} \to \mathfrak{B}$$

é elementar (ver Definição 4.8.11) se e somente se

$$(\mathfrak{A}, id_{|\mathfrak{A}|}) \equiv (\mathfrak{B}, \tau)$$

como $\mathcal{L}(\mathfrak{A})$-estruturas.

Em particular, para $\tau = id_{|\mathfrak{A}|}$

$$\mathfrak{A} \prec \mathfrak{B} \quad \textit{se, e somente se,} \quad (\mathfrak{A}, |\mathfrak{A}|) \equiv (\mathfrak{B}, |\mathfrak{A}|).$$

Prova. Na segunda parte do Lema 4.9.6 vemos que tomando $\sigma = \tau$, segue que τ é uma imersão elementar caso $(\mathfrak{B}, \tau)$ é um modelo de $Th_{\mathcal{L}(\mathfrak{A})}(\mathfrak{A}, |\mathfrak{A}|)$, o que é equivalente a $(\mathfrak{A}, |\mathfrak{A}|) \equiv (\mathfrak{B}, \tau)$.

Reciprocamente, se τ é uma imersão elementar e φ' uma $\mathcal{L}(\mathfrak{A})$-sentença, podemos pensar nesta sentença como obtida através de uma substituição

das variáveis $v_0, ..., v_n$ envolvidas em uma $\mathcal{L}$-fórmula φ por constantes $\underline{a_0}, ..., \underline{a_n}$. Assim

$$\varphi' = \varphi(v_0/\underline{a_0}, ..., v_n/\underline{a_n}).$$

Nisto utilizamos apenas as variáveis v_i as quais não aparecem em φ' para não haver problemas na substituição.

Suponha que

$$(\mathfrak{A}, id_{|\mathfrak{A}|}) \models \varphi',$$

então, pelo Lema 4.9.3

$$\mathfrak{A} \models \varphi[h],$$

para cada avaliação h com $h(v_i) = a_i$. Por hipótese a imersão τ é elementar, e temos portanto

$$\mathfrak{B} \models \varphi[\tau \circ h],$$

e novamente pelo Lema 4.9.3

$$(\mathfrak{B}, \tau) \models \varphi'.$$

Como isto vale para toda $\mathcal{L}(\mathfrak{A})$-sentença, concluímos que

$$(\mathfrak{A}, id_{|\mathfrak{A}|}) \equiv (\mathfrak{B}, \tau)$$

■

Agora extraímos uma consequência da primeira parte do Lema do Diagrama. Para isto introduzimos o conceito de subestrutura finitamente gerada a partir de um subconjunto A' do domínio de uma $\mathcal{L}$-estrutura $\mathfrak{A}$.

Não é difícil convencer-se que a intersecção dos domínios de qualquer quantidade de subestruturas de $\mathfrak{A}$ induz uma subestrutura de $\mathfrak{A}$ (lembramos que as relações e funções são interpretadas em cada subestrutura simplesmente como as restrições das relações e funções de $\mathfrak{A}$ a ela). Pela definição de subestrutura, as interpretações $c_k^{\mathfrak{A}}$ das constantes pertencem a cada domínio das subestruturas de $\mathfrak{A}$, e portanto $c_k^{\mathfrak{A}}$ pertence também à intersecção de todos.

Definição 4.9.9 *Chamamos uma tal subestrutura de subestrutura de intersecção, ou simplesmente de intersecção das subestruturas.*

Definição 4.9.10 *Dada uma $\mathcal{L}$-estrutura $\mathfrak{A}$ e um subconjunto não vazio $A' \subset |\mathfrak{A}|$, a subestrutura de $\mathfrak{A}$ gerada por A' é definida como a intersecção de todas as subestruturas de $\mathfrak{A}$ cujo domínio contém o conjunto A'. Uma subestrutura finitamente gerada de $\mathfrak{A}$ é a subestrutura de $\mathfrak{A}$ gerada por algum subconjunto finito $A' \subset |\mathfrak{A}|$.*

Com estas definições concluímos o

Corolário 4.9.11 *Sejam $\mathfrak{A}$ uma $\mathcal{L}$-estrutura e $\Sigma \subset Sent_{\mathcal{L}}$. Se toda subestrutura finitamente gerada de $\mathfrak{A}$ pode ser imersa em um modelo de Σ, então também $\mathfrak{A}$ pode ser imersa em um modelo de Σ.*

Prova. Pelo Lema 4.9.6 basta mostrar que o conjunto $\Sigma \cup D(\mathfrak{A})$ de $\mathcal{L}(\mathfrak{A})$-sentenças possui um modelo $(\mathfrak{B}, \sigma)$. Disto segue então que $\mathfrak{B}$ é um modelo de Σ e que $\mathfrak{A}$ é imersível em $\mathfrak{B}$.

Pelo Teorema da Finitude 4.4.15 basta mostrar que cada subconjunto finito Π de $\Sigma \cup D(\mathfrak{A})$ possui um modelo. Um tal conjunto pode conter apenas um número finito de sentenças $\delta_1, ..., \delta_n \in D(\mathfrak{A})$. Sejam $a_1, ..., a_m$ as novas constantes, com respeito a $\mathcal{L}$, que aparecem nas sentenças δ_i. Logo, pelas Definições 4.8.1 e 4.9.10, uma subestrutura finitamente gerada de $\mathfrak{A}$ é um modelo de $\{\delta_1, ..., \delta_n\}$. Por hipótese uma tal estrutura pode ser imersa em um Modelo $\mathfrak{C}$ de Σ. Por uma identificação, $\mathfrak{C}$ também é um modelo de $\Sigma \cup \{\delta_1, ..., \delta_n\}$, e portanto de Π.

■

Passamos agora a apresentar uma segunda construção de uma extensão elementar que não faz uso de uma ampliação da linguagem mas sim da noção de Cadeia Elementar de $\mathcal{L}$-estruturas. Este exemplo será utilizado na Seção 4.10 (veja Teorema 4.10.9).

Definição 4.9.12 *Uma sequência $(\mathfrak{A}_n)_{n\in\mathbb{N}}$ de $\mathcal{L}$-estruturas é dita uma cadeia elementar, se $\mathfrak{A}_{n+1}$ é uma extensão elementar de $\mathfrak{A}_n$, para cada $n \in \mathbb{N}$.*

Construímos no que segue, a partir de uma cadeia elementar $(\mathfrak{A}_n)_{n\in\mathbb{N}}$ de $\mathcal{L}$-estruturas, a estrutura união

$$\bigcup_{n\in\mathbb{N}}\mathfrak{A}_n,$$

e mostramos que ela é uma extensão elementar de cada $\mathfrak{A}_n$. Mais geralmente, consideraremos não apenas uma cadeia ordenada pelos naturais, mas também cadeias ordenadas por um número ordinal α. Salientamos que não exigimos, na definição a seguir, que as extensões sejam elementares:

Definição 4.9.13 *Uma seqüência $(\mathfrak{A}_\nu)_{\nu<\alpha}$ de $\mathcal{L}$-estruturas é dita uma α-cadeia , se*

$$\mathfrak{A}_\nu \subset \mathfrak{A}_\mu,$$

para todos ordinais ν, μ que satisfazem $\nu < \mu < \alpha$.

Neste caso, a estrutura união da $\alpha-$cadeia $(\mathfrak{A}_\nu)_{\nu<\alpha}$ é a $\mathcal{L}$-estrutura denotada por

$$\mathfrak{A} = \bigcup_{\nu<\alpha}\mathfrak{A}_\nu$$

e definida da seguinte maneira:

(i) $|\mathfrak{A}| = \bigcup_{\nu<\alpha}|\mathfrak{A}_\nu|$;

(ii) para todo $i \in I$, e todo $a_1, ..., a_{\lambda(i)} \in |\mathfrak{A}|$, digamos, $a_1, ..., a_{\lambda(i)} \in |\mathfrak{A}_\nu|$,

$$R_i^{\mathfrak{A}}(a_1, ..., a_{\lambda(i)}) \quad \text{se e só se} \quad \text{existe } \nu < \alpha \text{ tal que } R_i^{\mathfrak{A}_\nu}(a_1, ..., a_{\lambda(i)})$$

(iii) para todo $j \in J$, e todo $a_1, ..., a_{\mu(j)} \in |\mathfrak{A}|$, digamos, $a_1, ..., a_{\lambda(i)} \in |\mathfrak{A}_\nu|$, existe $\nu < \alpha$ tal que

$$f_j^{\mathfrak{A}}(a_1, ..., a_{\mu(j)}) = f_j^{\mathfrak{A}_\nu}(a_1, ..., a_{\mu(j)})$$

(iv) para todo $k \in K$ e para todo $\nu < \alpha$,

$$c_k^{\mathfrak{A}} = c_k^{\mathfrak{A}_\nu}.$$

Observe que, no caso de os números ordinais α e β satisfazerem $\alpha = \beta + 1$, temos

$$\bigcup_{\nu<\alpha} \mathfrak{A}_\nu = \mathfrak{A}_\beta,$$

ou seja, neste caso a união é igual ao maior termo da cadeia. De fato , como $\beta < \beta + 1$ obviamente temos

$$\mathfrak{A}_\beta \subset \bigcup_{\nu<\alpha} \mathfrak{A}_\nu.$$

Para a recíproca, salientamos que toda fórmula e todo termo são escritos com um número finito de parâmetros de $\bigcup_{\nu<\alpha} \mathfrak{A}_\nu$, ou seja de apenas alguns $\mathfrak{A}_{\nu_1}, ..., \mathfrak{A}_{\nu_r}$ com $\nu_1, ..., \nu_r < \beta + 1$. Como vale

$$\nu_i < \beta + 1 \Rightarrow \nu_i \leq \beta,$$

temos $\mathfrak{A}_{\nu_1}, ..., \mathfrak{A}_{\nu_r} \subset \mathfrak{A}_\beta$, e portanto

$$\bigcup_{\nu<\alpha} \mathfrak{A}_\nu \subset \mathfrak{A}_\beta.$$

Teorema 4.9.14 *Sejam α um número ordinal e $(\mathfrak{A}_\nu)_{\nu<\alpha}$ uma α-cadeia de $\mathcal{L}$-estruturas. Se,*

- para $\beta + 1 < \alpha$ vale $\mathfrak{A}_\beta \prec \mathfrak{A}_{\beta+1}$ e se

- para todo número ordinal limite $\lambda < \alpha$ vale $\mathfrak{A}_\lambda = \bigcup_{\nu<\lambda} \mathfrak{A}_\nu$,

então a união $\mathfrak{A} = \bigcup_{\nu<\alpha} \mathfrak{A}_\nu$ é uma extensão elementar de $\mathfrak{A}_\mu$ para cada $\mu < \alpha$.

Em particular, $\mathfrak{A}_0 \prec \mathfrak{A}$.

Prova. Faremos uma prova por indução ordinal sobre o comprimento α da cadeia.

- Se $\alpha = 0$, a cadeia é formada por um só elemento e a afirmação é trivial .

- Se α é um ordinal sucessor, digamos, $\alpha = \beta + 1$ e a $\alpha-$cadeia $(\mathfrak{A}_\nu)_{\nu<\alpha}$ satisfaz as hipóteses do teorema, então a $\beta-$cadeia $(\mathfrak{A}_\nu)_{\nu<\beta}$ também satisfaz

as hipóteses do teorema e portanto, pela hipótese de indução,

$$\mathfrak{A}_\mu \prec \bigcup_{\nu<\beta} \mathfrak{A}_\nu$$

para todo $\mu < \beta$, faltando-nos apenas mostrar que

$$\bigcup_{\nu<\beta} \mathfrak{A}_\beta \prec \mathfrak{A}_\beta, \tag{96}$$

uma vez que, pela observação acima,

$$\mathfrak{A}_\beta = \bigcup_{\nu<\beta+1} \mathfrak{A}_\nu = \bigcup_{\nu<\alpha} \mathfrak{A}_\nu.$$

pois daí, pela transitividade da relação $\prec$, também valerá

$$\mathfrak{A}_\mu \prec \bigcup_{\nu<\alpha} \mathfrak{A}_\nu$$

para todo $\mu < \alpha$.

- Se β for um ordinal limite, então, pela hipótese,

$$\bigcup_{\nu<\beta} \mathfrak{A}_\nu = \mathfrak{A}_\beta,$$

e (96) segue trivialmente.

- Se β for um ordinal sucessor, digamos, $\beta = \gamma + 1$, então, novamente pela observação acima,

$$\bigcup_{\nu<\beta} \mathfrak{A}_\nu = \bigcup_{\nu<\gamma+1} \mathfrak{A}_\nu = \mathfrak{A}_\gamma,$$

e como $\gamma + 1 = \beta < \alpha$, vale pela hipótese que

$$\mathfrak{A}_\gamma \prec \mathfrak{A}_{\gamma+1} = \mathfrak{A}_\beta,$$

e portanto vale (96).

- Se α é um ordinal limite, por hipótese, pela hipótese de indução e pela

observação acima, temos que, neste caso,

$$\mathfrak{A}_\mu \prec \mathfrak{A}_\nu$$

sempre que $\mu < \nu < \alpha$, e queremos então mostrar que $\mathfrak{A}_\mu \prec \mathfrak{A}$ para todo $\mu < \alpha$. Para isto, provamos, por indução sobre a construção da fórmula φ, a equivalência

$$\mathfrak{A}_\mu \models \varphi[h] \quad \text{se e só se} \quad \mathfrak{A} \models \varphi[h],$$

para todo $\mu < \alpha$ e para toda avaliação h em $\mathfrak{A}_\mu$.

Como já sabemos que existe uma imersão (pela construção da $\alpha-$cadeia), já vimos anteriormente que esta indução é rotineira até o passo de transmitir a não validade de uma fórmula $\forall x\ \psi$ pela avaliação h em $\mathfrak{A}$ para $\mathfrak{A}_\mu$.

Suponhamos então

$$\mathfrak{A} \not\models \forall x\ \psi[h].$$

Isto significa que existe um $a \in |\mathfrak{A}|$ com

$$\mathfrak{A} \not\models \psi[h(x, a)].$$

Sejam $Fr(\psi) \subset \{v_0, ..., v_n\}$ e denotemos por $a_i = h(v_i)$ para $0 \leq i \leq n$. Como $|\mathfrak{A}|$ é uma união de conjuntos totalmente ordenados, $a, a_0, ..., a_n$ já se encontram em algum membro desta união, digamos $|\mathfrak{A}_\nu|$ e, sem perda de generalidade, podemos supor $\mu < \nu$. Para a fórmula ψ e a avaliação $h(x, a)$ em $\mathfrak{A}_\nu$ segue agora por hipótese de indução (sobre o comprimento das fórmulas), que

$$\mathfrak{A}_\nu \not\models \psi[h(x, a)].$$

Disto resulta, em particular,

$$\mathfrak{A}_\nu \not\models \forall x\ \psi[h].$$

E como $\mathfrak{A}_\mu \prec \mathfrak{A}_\nu$ pela hipótese de indução (sobre α) obtemos finalmente

$$\mathfrak{A}_\mu \not\models \forall x\ \psi[h].$$

■

Observação 4.9.15 *No caso de uma ω-cadeia,*

$$(\mathfrak{A}_\nu)_{\nu<\omega} = (\mathfrak{A}_n)_{n\in\mathbb{N}},$$

não estão envolvidos números ordinais limites. Neste caso, a hipótese do teorema acima resume-se apenas à condição $\mathfrak{A}_n \prec \mathfrak{A}_{n+1}$ para todo $n \in \mathbb{N}$.

Definição 4.9.16 *Uma α-cadeia elementar é uma α-cadeia que satisfaz as hipóteses do Teorema 4.9.14.*

Se uma cadeia não for elementar , então a validade de uma sentença não se transmite em geral para a união. No entanto, para algumas sentenças especiais (mais simples) isto não ocorre.

Observação 4.9.17 *Sejam α um número ordinal e $(\mathfrak{A}_\nu)_{\nu<\alpha}$ uma α-cadeia de $\mathcal{L}$-estruturas. Se uma $\forall\exists$-sentença φ vale em cada membro da cadeia $\mathfrak{A}_\nu$, então também vale na união $\bigcup_{\nu<\alpha} \mathfrak{A}_\nu = \mathfrak{A}$. Por uma $\forall\exists$-sentença entendemos uma sentença da forma*

$$\forall x_1, ..., x_n \; \exists y_1, ..., y_m \; \psi,$$

onde ψ é livre de quantificadores. A prova desta afirmação pode ser encontrada em [11], pag 120

O mesmo no entanto não ocorre para $\exists\forall$-sentenças. Por exemplo, sejam

$$\mathfrak{A}_n = \left\langle \frac{1}{n!}\,\mathbb{Z}; <_n \right\rangle,$$

onde para cada $n \in \mathbb{N}$

$$\frac{1}{n!}\,\mathbb{Z} = \left\{ \frac{m}{n!} \mid m \in \mathbb{Z} \right\}$$

e $<_n$ é a restrição da ordem de $\mathbb{Q}$ sobre este conjunto. É claro que $(\mathfrak{A}_n)_{n<\omega}$ é uma ω-cadeia. Em cada termo $\mathfrak{A}_n$ da cadeia vale a $\exists\forall$-sentença

$$\exists x \; \forall y \; (0 < x \wedge \; (y < 0 \vee x = y \vee x < y)).$$

Para cada $\frac{1}{n!}\mathbb{Z}$ tem-se $\frac{1}{n!}$ como este menor elemento positivo. Esta sentença contudo não vale em

$$\bigcup_{n<\omega} \mathfrak{A}_n = \langle \mathbb{Q}; <^{\mathbb{Q}} \rangle.$$

4.10 Estruturas saturadas

Um problema típico da Teoria de Modelos é, a partir de uma estrutura dada, construir uma estrutura elementarmente equivalente a ela e satisfazendo condições adicionais como, por exemplo, condições sobre a cardinalidade desta nova estrutura.

Introduzimos nesta seção um conceito fundamental para a Teoria dos Modelos e para este texto: o conceito de estrutura saturada. A existência, e num certo sentido unicidade de uma extensão elementar saturada de uma dada estrutura infinita é muito útil para a análise da sua Teoria, como veremos no caso da teoria dos corpos valorizados no próximo Capítulo.

Voltamos aqui a considerar a extensão da linguagem $\mathcal{L}$ pelo acréscimo de constantes $\underline{a}$ para $a \in A'$, onde A' é um subconjunto de $|\mathfrak{A}|$.

Notação 4.10.1 *Dado um conjunto de fórmulas Φ, escreveremos $\Phi(v_0) = \Phi$ para indicar que $Fr(\varphi) \subseteq \{v_0\}$ para toda $\varphi \in \Phi$.*

Definição 4.10.2 *Sejam $\mathfrak{A}$ uma $\mathcal{L}$-estrutura e A' um subconjunto de $|\mathfrak{A}|$. Um conjunto de $\mathcal{L}(A')$-fórmulas $\Phi(v_0)$ é dito um Tipo (elementar) de $\mathfrak{A}$, (mais precisamente um tipo de $(\mathfrak{A}, A')$), caso exista uma extensão elementar $\mathfrak{A}_1$ de $\mathfrak{A}$, como $\mathcal{L}$-estruturas, e um $a \in A_1 = |\mathfrak{A}_1|$ tal que para todo $\varphi \in \Phi$ as $\mathcal{L}(A_1)$-sentenças $\varphi(\underline{a})$ valem na $\mathcal{L}(A_1)$-estrutura $(\mathfrak{A}_1, A_1)$, ou seja:*

$$(\mathfrak{A}_1, A_1) \models \varphi(\underline{a})$$

Escrevemos também neste caso

$$(\mathfrak{A}_1, A_1) \models \Phi(\underline{a}),$$

e dizemos que $\Phi(v_0)$ é realizável, ou satisfeito, em $(\mathfrak{A}_1, A_1)$ por a.

Observação 4.10.3 *Observamos que, pelo fato de φ ser uma $\mathcal{L}(A')$-fórmula, para fazer sentido*

$$(\mathfrak{A}_1, A_1) \models \varphi(\underline{a})$$

é necessário que as interpretações das constantes $\underline{a'}$ que aparecem em φ, com $a' \in A'$, façam sentido em $(\mathfrak{A}_1, A_1)$. Isto está garantido, por exemplo, se $A' \subseteq A_1$ e interpretamos $\underline{a'}$ como o próprio $a' \in A'$.

Outro fato importante de ser lembrado aqui é a segunda conquência do Corolário 4.9.8:

$$\mathfrak{A} \prec \mathfrak{A}_1 \quad \textit{se, e somente se,} \quad (\mathfrak{A}, |\mathfrak{A}|) \equiv (\mathfrak{A}_1, |\mathfrak{A}|).$$

Notação 4.10.4 *De agora em diante escreveremos simplesmente*

$$\psi(c_1, ..., c_n)$$

para significar $\psi(x_1/c_1, ..., x_n/c_n)$ quando estiver claro através de quais variáveis estamos substituindo as constantes.

Antes de enunciarmos o próximo resultado, salientamos que se $\Phi(v_0)$ é realizável em $(\mathfrak{A}_1, A_1)$ por a_1 e é também um conjunto finito, digamos,

$$\Phi(v_0) = \{\varphi_1, ..., \varphi_n\},$$

isto significa que,

$$(\mathfrak{A}_1, A_1) \models \varphi_i(a_1), \ i \in \{1, 2, ..., n\},$$

ou equivalentemente,

$$(\mathfrak{A}_1, A_1) \models \exists v_0 \ (\varphi_1 \wedge ... \wedge \varphi_n).$$

Em geral, quando $\Phi(v_0)$ é infinito, não podemos juntar todas as fórmulas e formar, por exemplo,

$$\bigwedge_{i=1}^{\infty} \varphi_i(v_0)$$

pois não temos aí uma sentença, mas podemos ainda afirmar que

$$(\mathfrak{A}, A) \models \exists v_0 \, \varphi(v_0),$$

para todo $\varphi \in \Phi(v_0)$.

Lema 4.10.5 *Sejam $\mathfrak{A}$ uma $\mathcal{L}$-estrutura e $A = |\mathfrak{A}|$. Um conjunto $\Phi(v_0)$ de $\mathcal{L}(A)$-fórmulas é um tipo de $\mathfrak{A}$ se, e somente se, cada subconjunto finito $\{\varphi_1, ..., \varphi_n\}$ de $\Phi(v_0)$ é realizável em $(\mathfrak{A}, A)$, ou seja,*

$$(\mathfrak{A}, A) \models \exists v_0 \, (\varphi_1 \wedge ... \wedge \varphi_n).$$

Prova. Suponhamos que $\Phi(v_0)$ é um Tipo de $\mathfrak{A}$ e seja $\mathfrak{A} \prec \mathfrak{A}_1$ (como $\mathcal{L}$-estruturas) tal que

$$(\mathfrak{A}_1, A_1) \models \Phi(\underline{a})$$

para um $a \in A_1 = |\mathfrak{A}_1|$. Então, para todo subconjunto finito $\{\varphi_1, ..., \varphi_n\}$ de $\Phi(v_0)$ vale

$$(\mathfrak{A}_1, A_1) \models \exists v_0 \, (\varphi_1 \wedge ... \wedge \varphi_n).$$

Afirmamos que também

$$(\mathfrak{A}_1, A) \models \exists v_0 \, (\varphi_1 \wedge ... \wedge \varphi_n).$$

De fato, inicialmente salientamos que esta afirmação faz sentido, pois $\varphi_1, ..., \varphi_n$ são $\mathcal{L}(A)$-fórmulas. Como $\mathfrak{A} \prec \mathfrak{A}_1$, pelo Corolário 4.9.8

$$(\mathfrak{A}_1, A) \equiv (\mathfrak{A}, A).$$

Em particular para a $\mathcal{L}(A)$-sentença $\exists v_0 \, (\varphi_1 \wedge ... \wedge \varphi_n)$ temos

$$(\mathfrak{A}, A) \models \exists v_0 \, (\varphi_1 \wedge ... \wedge \varphi_n).$$

Reciprocamente, suponhamos que cada subconjunto finito de $\Phi(v_0)$ é realizável em $(\mathfrak{A}, A)$.

Consideramos então o conjunto de $\mathcal{L}(A \cup \{c\})$-sentenças

$$\Sigma = Th_{\mathcal{L}(A)}(\mathfrak{A}, A) \cup \Phi(c),$$

onde c é uma nova constante e $\Phi(c) = \{\varphi(c) \mid \varphi \in \Phi(v_0)\}$.

Até aqui então;

- $\Phi(v_0)$ é um conjunto de $\mathcal{L}(A)$-fórmulas.
- $\Phi(c)$ é um conjunto de $\mathcal{L}(A \cup \{c\})$-sentenças.

Afirmamos que cada subconjunto finito de Σ possui um modelo. De fato, um tal subconjunto está contido em um conjunto da forma

$$Th_{\mathcal{L}(A)}(\mathfrak{A}, A) \cup \{\varphi_1(c), ..., \varphi_n(c)\}$$

para alguns $\varphi_1, .., \varphi_n \in \Phi(v_0)$. Por hipótese, $\{\varphi_1, .., \varphi_n\}$ é realizável em $(\mathfrak{A}, A)$, ou seja:

$$(\mathfrak{A}, A) \models \exists v_0(\varphi_1(v_0) \wedge ... \wedge \varphi_n(v_0)),$$

e portanto, denotando por a um elemento de $A = |\mathfrak{A}|$ tal que

$$(\mathfrak{A}, A) \models (\varphi_1(\underline{a}) \wedge ... \wedge \varphi_n(\underline{a})),$$

ao interpretarmos a nova constante c como a (isto é tomamos $c^{(\mathfrak{A},A)} = a$), temos que $(\mathfrak{A}, A)$ é um modelo para $Th_{\mathcal{L}(A)}(\mathfrak{A}, A) \cup \{\varphi_1(c), ..., \varphi_n(c)\}$.

Assim, pelo Teorema da Finitude 4.4.15, existe uma $\mathcal{L}(A \cup \{c\})$-estrutura que é um modelo para Σ. Denotemos tal estrutura por $\mathfrak{A}_1$.

Ora, mas então tal estrutura é, em particular, um modelo para

$$Th_{\mathcal{L}(\mathfrak{A})}(\mathfrak{A}, A).$$

O Lema do Diagrama 4.9.6 nos garante então que $\mathfrak{A}_1$ é uma extensão elementar de $\mathfrak{A}$ (identificando $\mathfrak{A}$ com sua imagem em $\mathfrak{A}_1$). Denotando por b a interpretação $c^{\mathfrak{A}_1} \in |\mathfrak{A}_1|$, segue que

$$(\mathfrak{A}_1, A \cup \{b\}) \models \Phi(c),$$

e obtemos

$$(\mathfrak{A}_1, A_1) \models \Phi(\underline{b}),$$

uma vez que $A_1 \supseteq A \cup \{b\}$. Ou seja, $\Phi(v_0)$ é um tipo de $\mathfrak{A}$.

■

Observação 4.10.6 *Em geral, mesmo quando cada subconjunto finito de um Tipo $\Phi(v_0)$ de $\mathfrak{A}$ é realizável em $(\mathfrak{A}, A)$, ainda pode não ocorrer*

$$(\mathfrak{A}, A) \models \exists v_0\ \Phi(v_0),$$

isto é, o Tipo não ser realizável dentro da própria $\mathfrak{A}$, sendo mesmo necessário considerar uma extensão distinta de $\mathfrak{A}$.

O contra-exemplo mais simples é o seguinte: sejam $\mathfrak{A}$ uma estrutura infinita com $A = |\mathfrak{A}|$ e $\Phi(v_0) = \{v_0 \neq \underline{a} \mid a \in A\}$ um conjunto de $\mathcal{L}(A)$-fórmulas com variável livre v_0. Pela infinitude de A, é claro que cada subconjunto finito de $\Phi(v_0)$ é realizável em $(\mathfrak{A}, A)$. Contudo, obviamente $\Phi(v_0)$ não o é. Portanto, para o caso geral, precisamos sim de uma extensão de $(\mathfrak{A}, A)$, como enunciado no Lema.

Em uma estrutura $\mathfrak{A}$, que vamos definir como "κ-saturada" , somos capazes de realizar tantos tipos de $\mathfrak{A}$ quantos forem possíveis, respeitando uma certa limitação que depende de κ.

Definição 4.10.7 *Dado um número cardinal infinito κ chamamos uma $\mathcal{L}$-estrutura $\mathfrak{A}$ de κ-saturada, caso cada Tipo $\Phi(v_0)$ de $(\mathfrak{A}, A')$ com $\mathsf{card}(A') < \kappa$ puder ser realizado em $(\mathfrak{A}, A)$.*

Observação 4.10.8 *Por esta definição, toda estrutura finita é sempre κ-saturada. De fato, se $\mathfrak{A}$ é finita e $\Phi(v_0)$ é um tipo de $\mathfrak{A}$, então existe uma extensão elementar $\mathfrak{A}_1$ de $\mathfrak{A}$ na qual $\Phi(v_0)$ é realizável. Então, por $\mathfrak{A}_1$ ser elementarmente equivalente a $\mathfrak{A}$, e $\mathfrak{A}$ ser finita, pelo Teorema 4.7.5.*

$$\mathfrak{A}_1 \simeq \mathfrak{A},$$

e por tratar-se de extensão elementar, concluímos que

$$\mathfrak{A}_1 = \mathfrak{A}.$$

Para $A = |\mathfrak{A}|$ infinito obtemos da κ-saturação imediatamente

$$\kappa \leq \mathsf{card}(A),$$

pois caso contrário o Tipo $\{v_0 \neq \underline{a} \mid a \in A\}$ deveria ser realizável em $(\mathfrak{A}, A)$. Uma outra consequência é que cada estrutura $\mathfrak{A}$ que é κ-saturada também é κ'-saturada para cada número cardinal infinito $\kappa' \leq \kappa$. Mais ainda, a noção de κ-saturação é invariante por extensões com menos do que κ constantes.

Também é claro que Tipos de $\mathfrak{A}$ são conjuntos de fórmulas da linguagem $\mathcal{L}(A)$. As novas constantes deixam-se sempre ser substituídas por constantes $\underline{a}$ da linguagem $\mathcal{L}(A)$. (Observe que um elemento $a \in A$ além de $\underline{a}$, pode ser simbolizado por outras constantes).

Mostraremos agora que para toda estrutura infinita existe uma extensão elementar saturada. Lembramos para isto que o sucessor cardinal de κ será simbolizado por κ^+. Assim, $\kappa^+ \leq 2^\kappa$.

Teorema 4.10.9 (Teorema da Existência de Estrutura κ^+-Saturada) *Para cada número cardinal $\kappa \geq \kappa_\mathcal{L}$ e cada $\mathcal{L}$-estrutura infinita $\mathfrak{A}$ com $\mathsf{card}(|\mathfrak{A}|) \leq 2^\kappa$ existe uma κ^+-saturada extensão elementar $\mathfrak{A}^*$ com $\kappa^+ \leq \mathsf{card}(|\mathfrak{A}^*|) \leq 2^\kappa$.*

Prova. Construiremos uma κ^+-cadeia elementar $(\mathfrak{A}_\nu)_{\nu<\kappa^+}$ com $\mathfrak{A}_0 = \mathfrak{A}$ e com as seguintes propriedades:

(1) Para todo ordinal $\nu < \kappa^+$ temos $\mathsf{card}(A_\nu) \leq 2^\kappa$, onde $A_\nu = |\mathfrak{A}_\nu|$.

(2) Para um ordinal $\nu < \kappa^+$, a estrutura $\mathfrak{A}_{\nu+1}$ realiza todo tipo $\Phi(v_0)$ de $\mathfrak{A}_\nu$ com $\mathsf{card}(\Phi(v_0)) \leq \kappa$.

Começamos definindo

$$\mathfrak{A}_0 := \mathfrak{A}.$$

Supondo que já temos definidas as estruturas $\mathfrak{A}_\nu$ da cadeia elementar para todo $\nu < \lambda < \kappa^+$, com λ número ordinal limite, definimos

$$\mathfrak{A}_\lambda := \bigcup_{\nu<\lambda} \mathfrak{A}_\nu.$$

E, para definir $\mathfrak{A}_{\nu+1}$ supondo já definido o termo $\mathfrak{A}_\nu$ da cadeia, indexamos todos os tipos $\Phi(v_0)$ de $\mathfrak{A}_\nu$ com $\mathsf{card}(\Phi(v_0)) \leq \kappa$ por números ordinais $< 2^\kappa$, assim $(\Phi_\mu)_{\mu<2^\kappa}$ é o conjunto de todos os tipos de $\mathfrak{A}_\nu$.

Lembrando que todo Tipo de $\mathfrak{A}_\nu$ é um subconjunto de $Fml_{\mathcal{L}(A_\nu)}$, vemos que isto é possível. De fato, $\mathsf{card}(Fml_{\mathcal{L}(A_\nu)}) \leq 2^\kappa$, e com isto a cardinalidade de um conjunto de subconjuntos de $Fml_{\mathcal{L}(A_\nu)}$, que por sua vez têm cardinalidade $\leq \kappa$, pode ser estimada através da cardinalidade do conjunto de aplicações de κ em $Fml_{\mathcal{L}(A_\nu)}$. Verdadeiramente vale:

$$\mathsf{card}({}^\nu(Fml_{\mathcal{L}(A_\nu)})) \leq (2^\nu)^\nu = 2^{\nu.\nu} = 2^\nu.$$

Definimos então

$$\mathfrak{A}_{\nu+1} = \bigcup_{\mu<2^\kappa} \mathfrak{A}_\nu^{(\mu)},$$

onde a sequência $\mathfrak{A}_\nu^{(\mu)}$ é estipulada da seguinte forma:

$$\begin{aligned}
\mathfrak{A}_\nu^{(0)} &= \mathfrak{A}_\nu; \\
\mathfrak{A}_\nu^{(\lambda)} &= \bigcup_{\mu<\lambda} \mathfrak{A}_\nu^{(\mu)}, \text{ para números ordinais limite } \lambda < 2^\kappa; \\
\mathfrak{A}_\nu^{(\mu+1)} &= \text{uma extensão elementar } \mathfrak{B} \text{ de } \mathfrak{A}_\nu^{(\mu)}, \\
&\quad \text{a qual realiza } \Phi_\mu(v_0) \text{ com } \mathsf{card}(B) \leq 2^\kappa.
\end{aligned}$$

A existência de uma tal extensão elementar $\mathfrak{B}$ segue imediatamente da definição de um Tipo de $\mathfrak{A}_\nu^{(\mu)}$ junto com o Teorema 4.8.8 escolhendo $\mathfrak{C} = \mathfrak{A}_\nu$.

Logo, pelo Teorema 4.9.14, segue que $\mathfrak{A}_{\nu+1}$ é uma extensão elementar de $\mathfrak{A}_\nu$.

A condição (2) é obviamente satisfeita, pois para um Tipo $\Phi(v_0)$ de

$\mathfrak{A}_\nu$ com $\mathsf{card}(\Phi(v_0)) \leq \kappa$, existe um $\mu < 2^\kappa$ com $\Phi(v_0) = \Phi_\mu(v_0)$, e pela construção existe um $a \in A_\nu^{(\mu+1)}$ que realiza $\Phi(v_0)$ em $\mathfrak{A}_\nu^{(\mu+1)}$. Por termos $\mathfrak{A}_\nu^{(\mu+1)} \prec \mathfrak{A}_{\nu+1}$ (novamente Teorema 4.9.14), vale também

$$(\mathfrak{A}_{\nu+1}, A_{\nu+1}) \models \Phi(\underline{a}).$$

A condição (1) segue de

$$\mathsf{card}(A_{\nu+1}) = \mathsf{card}(\bigcup_{\mu<2^\kappa} A_\nu^{(\mu)}) \leq \max(2^\kappa, 2^\kappa) = 2^\kappa.$$

E, para o caso de $\mathfrak{A}_\lambda = \bigcup_{\nu<\lambda} \mathfrak{A}_\nu$, com λ ordinal limite satisfazendo $\lambda < \kappa^+ \leq 2^\kappa$, desigualdades análogas nos levam a

$$\mathsf{card}(A_\lambda) = \mathsf{card}(\bigcup_{\nu<\lambda} A_\nu) \leq \max(2^\kappa, \lambda) = 2^\kappa.$$

Uma vez construída a κ^+-cadeia elementar, definimos $\mathfrak{A}_{\kappa^+} =: \mathfrak{A}^*$ a união desta cadeia. Do Teorema 4.9.14 concluímos que $\mathfrak{A}^*$ é uma extensão elementar de $\mathfrak{A}$. Segue de (1) que, se $A^* = |\mathfrak{A}^*|$ então

$$\mathsf{card}(A^*) = \mathsf{card}(\bigcup_{\nu<\kappa^+} A_\nu) \leq \max(\kappa^+, 2^\kappa) = 2^\kappa.$$

Finalmente vamos mostrar que $\mathfrak{A}^*$ é κ^+-saturada.

Seja $\Phi(v_0)$ um tipo de $(\mathfrak{A}^*, A')$ com $\mathsf{card}(A') \leq \kappa$, então segue da regularidade do número cardinal sucessor κ^+ que $A' \subset A_\nu$ para um $\nu < \kappa^+$. De $\mathfrak{A}_\nu \prec \mathfrak{A}^*$, segue que $\Phi(v_0)$ é um tipo de $\mathfrak{A}_\nu$. Por (2) e por

$$\mathsf{card}(\Phi) \leq \max(\kappa_{\mathcal{L}}, \mathsf{card}(A')) \leq \kappa,$$

existe um elemento $a \in A_{\nu+1}$ que realiza este tipo em $\mathfrak{A}_{\nu+1}$, ou seja,

$$(\mathfrak{A}_{\nu+1}, A_{\nu+1}) \models \Phi(\underline{a})$$

Isto porém implica $(\mathfrak{A}^*, A^*) \models \Phi(\underline{a})$, pois $\mathfrak{A}_{\nu+1} \prec \mathfrak{A}^*$.

■

Definição 4.10.10 *Uma $\mathcal{L}$-estrutura infinita $\mathfrak{A}$ é dita saturada quando for $\mathsf{card}(|\mathfrak{A}|)$-saturada.*

Supondo anteriormente a *hipótese do contínuo universal*, que diz que $2^\kappa = \kappa^+$ para todo κ número cardinal infinito, então o Teorema 4.10.9 nos diz que para cada estrutura infinita $\mathfrak{A}$ e cada sucessor cardinal κ^+ tais que

$$\max(\kappa_{\mathcal{L}}^+, \mathsf{card}(|\mathfrak{A}|)) \leq \kappa^+,$$

existe uma extensão elementar *saturada* de cardinalidade κ^+. Esta estrutura, como provaremos no Teorema do Isomorfismo (Teorema 4.10.17), é determinada univocamente a menos de isomorfismos.

Antes provamos o Teorema da Imersão que utiliza a seguinte definição:

Definição 4.10.11 *Uma $\mathcal{L}$-sentença é dita existencial ou uma $\exists$-sentença quando tiver a forma*

$$\exists x_1, ..., x_n \ \delta,$$

com δ livre de quantificadores. Consideramos também as sentenças livres de quantificadores como existenciais.

Notação 4.10.12 *Dadas duas $\mathcal{L}$-estruturas $\mathfrak{A}$ e $\mathfrak{A}'$, quando a validade de cada $\exists$-sentença de $\mathfrak{A}$ transfere-se para $\mathfrak{A}'$, ou equivalentemente,*

$$\mathfrak{A} \models \varphi \text{ implica } \mathfrak{A}' \models \varphi,$$

para toda $\mathcal{L}$-sentença existencial φ, escrevemos resumidamente

$$\mathfrak{A} \overset{\exists}{\rightsquigarrow} \mathfrak{A}'$$

para este fato. Utilizamos esta maneira de escrita também numa extensão da linguagem $\mathcal{L}$.

Teorema 4.10.13 (Teorema da Imersão) *: Sejam $\mathfrak{A}$ e $\mathfrak{A}'$ duas $\mathcal{L}$-estruturas tais que*

(i) $\mathfrak{A}'$ é κ-saturada, sendo κ um número cardinal infinito.

(*ii*) $\kappa \geq \mathsf{card}(|\mathfrak{A}|)$.

(*iii*) *Toda* $\exists$*-sentença que vale em* $\mathfrak{A}$ *também vale em* $\mathfrak{A}'$.

Então $\mathfrak{A}$ *pode ser imersa em* $\mathfrak{A}'$.

Prova. Seja $\alpha = \mathsf{card}(A)$, onde $A = |\mathfrak{A}|$. Escolhemos uma bijeção de α em A, a qual nos fornece uma indexação $(a_\nu)_{\nu<\alpha}$ dos elementos de A. Construiremos uma sequência ordinal $(a'_\nu)_{\nu<\alpha}$ de elementos de $A' = |\mathfrak{A}'|$, tal que

$$(\mathfrak{A}, (a_\nu)_{\nu<\alpha}) \overset{\exists}{\rightsquigarrow} (\mathfrak{A}', (a'_\nu)_{\nu<\alpha}). \qquad (*)$$

A linguagem $\mathcal{L}_\alpha$ desta extensão é precisamente uma extensão por constantes c_ν com $\nu < \alpha$, onde supomos que $K \cap \{\nu \mid \nu < \alpha\} = \emptyset$.

No decorrer da prova consideramos extensões por constantes $\mathcal{L}_\beta$ de $\mathcal{L}$, para todo $\beta \leq \alpha$, de modo totalmente análogo.

Supondo construída tal sequência com a propriedade $(*)$, temos em particular que todas as sentenças do Diagrama $D(\mathfrak{A})$ que valem em $(\mathfrak{A}, (a_\nu)_{\nu<\alpha})$ também valem em $(\mathfrak{A}', (a'_\nu)_{\nu<\alpha})$, por serem livres de quantificadores.

Como claramente $(\mathfrak{A}, (a_\nu)_{\nu<\alpha}) \equiv (\mathfrak{A}, |\mathfrak{A}|)$, temos que $(\mathfrak{A}', (a'_\nu)_{\nu<\alpha})$ é também um modelo de $D(\mathfrak{A})$. Pelo Lema do Diagrama 4.9.6, $\mathfrak{A}$ é imersível em $\mathfrak{A}'$ como desejávamos.

Passamos agora à construção da sequência mencionada. Construiremos a sequência $(a'_\nu)_{\nu<\alpha}$ de modo que vale para todo $\beta < \alpha$:

$$(\mathfrak{A}, (a_\nu)_{\nu\leq\beta}) \overset{\exists}{\rightsquigarrow} (\mathfrak{A}', (a'_\nu)_{\nu\leq\beta}). \qquad (*)_\beta$$

Afirmamos que desta propriedade segue imediatamente que esta sequência satisfaz $(*)$. Mostramos isto por indução ordinal:

- Para o caso em que α é um número cardinal finito isto é imediatamente claro.

- Se α é um número cardinal infinito, então α é um número ordinal limite.

Neste caso, toda $\exists$-sentença φ da linguagem $\mathcal{L}_\alpha$ envolve apenas um número finito de constantes c_ν, e por isso φ já é uma $\exists$-sentença da linguagem $\mathcal{L}_\beta$ para algum $\beta < \alpha$. Assim obtemos da hipótese $(*)_\beta$ que

$$(\mathfrak{A}, (a_\nu)_{\nu<\alpha}) \models \varphi$$

implica

$$(\mathfrak{A}', (a'_\nu)_{\nu<\alpha}) \models \varphi.$$

Finalmente, passamos para a definição da sequência $(a'_\nu)_{\nu<\alpha}$. Seja $\gamma < \alpha$. Supomos que a sequência $(a'_\nu)_{\nu<\alpha}$ já esta definida para todo $\beta < \gamma$ e que $(*)_\beta$ valha. Precisamos portanto encontrar para a_γ um $a'_\gamma \in A'$ tal que $(*)_\gamma$ valha.

Seja $\exists\Delta(v_0)$ o conjunto de todas as $\exists$-fórmulas[8] φ da linguagem $\mathcal{L}_\gamma$ com $Fr(\varphi) \subset \{v_0\}$ e com

$$(\mathfrak{A}, (a_\nu)_{\nu\leq\gamma}) \models \varphi(c_\gamma).$$

Indiscutivelmente $\Phi(v_0) = \exists\Delta(v_0)$ é um Tipo de $(\mathfrak{A}, (a_\nu)_{\nu<\gamma})$. Pelo Lema 4.10.5, para cada subconjunto $\{\varphi_1, ..., \varphi_n\}$ de $\Phi(v_0)$ nós temos

$$(\mathfrak{A}, (a_\nu)_{\nu<\gamma}) \models \exists v_0\ (\varphi_1 \wedge ... \wedge \varphi_n).$$

Seja β o máximo dos índices das constantes c_ν que aparecem em $\exists v_0\ (\varphi_1 \wedge ... \wedge \varphi_n)$. É óbvio que $\beta < \gamma$ e com isto $\exists v_0\ (\varphi_1 \wedge ... \wedge \varphi_n)$ é uma $\exists$-sentença da linguagem $\mathcal{L}_{\beta+1}$. Pela hipótese $(*)_\beta$ temos com isto também

$$(\mathfrak{A}', (a'_\nu)_{\nu<\gamma}) \models \exists v_0\ (\varphi_1 \wedge ... \wedge \varphi_n).$$

Assim, novamente pelo Lema 4.10.5, $\Phi(v_0)$ é também um tipo de

$$(\mathfrak{A}', (a'_\nu)_{\nu<\gamma}).$$

Como todo Tipo de $(\mathfrak{A}', (a'_\nu)_{\nu<\gamma})$ é um Tipo de $\mathfrak{A}'$ (veja Definição 4.10.2),

[8]Uma $\exists$-fórmula é entendida como uma fórmula que, ao substituir suas variáveis livres por constantes, obtemos uma $\exists$-sentença.

da κ-saturabilidade de $\mathfrak{A}'$ obtemos a κ-saturabilidade de $(\mathfrak{A}', (a'_\nu)_{\nu<\gamma}) = \mathfrak{A}''$. (veja Definição 4.10.7)

Portanto, por $\mathsf{card}(\gamma) < \alpha \leq \kappa$ e pela κ-saturação de $\mathfrak{A}''$, o Tipo $\Phi(v_0)$ é realizável em $(\mathfrak{A}'', |\mathfrak{A}''|)$, ou seja, existe um $a'_\gamma \in A' = |\mathfrak{A}''|$ com $(\mathfrak{A}', (a'_\nu)_{\nu\leq\gamma}) \models \Phi(c_\gamma)$.

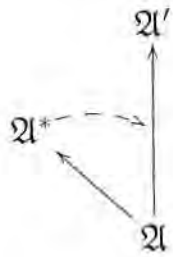
Com isto mostramos precisamente $(*)_\gamma$. De fato, se φ é uma $\exists$-sentença da forma $\exists x_1, ..., x_n\ \delta$, com δ livre de quantificadores, podemos supor, sem perda de generalidade, no caso em que φ envolve a constante c_γ que $v_0 \notin \{x_1, ..., x_n\}$ e obter com isto $\varphi = \varphi(c_\gamma/v_0)(v_0/c_\gamma)$. Tomamos então $\Phi(v_0) = \{\varphi(c_\gamma/v_0)\}$.

■

Antes do teorema dos isomorfismos mostramos ainda algumas consequências.

Definição 4.10.14 *Dizemos que uma $\mathcal{L}$-subestrutura $\mathfrak{A}$ de $\mathfrak{A}'$ é existencialmente fechada em $\mathfrak{A}'$, se toda sentença existencial da linguagem $\mathcal{L}(\mathfrak{A})$ que vale em $(\mathfrak{A}', |\mathfrak{A}|)$ também vale em $(\mathfrak{A}, |\mathfrak{A}|)$.*

Corolário 4.10.15 *Sejam $\mathfrak{A}, \mathfrak{A}^*$ e $\mathfrak{A}'$ $\mathcal{L}$-estruturas tais que $\mathfrak{A}$ é uma $\mathcal{L}$-subestrutura comum das $\mathcal{L}$-estruturas $\mathfrak{A}^*$ e $\mathfrak{A}'$ e sejam $A = |\mathfrak{A}|$ e $A^* = |\mathfrak{A}^*|$.*



(1) *Se $\mathfrak{A}'$ é κ-saturada com $\kappa > \mathsf{card}(|\mathfrak{A}^*|)$ e*

   (a) *$\mathfrak{A}$ é existencialmente fechada em $\mathfrak{A}^*$, ou*

   (b) *cada $\mathcal{L}(A)$-subestrutura finitamente gerada de $\mathfrak{A}^*$ pode ser imersa em $\mathfrak{A}'$,*

então $\mathfrak{A}^*$ pode ser imersa em $\mathfrak{A}'$ como uma $\mathcal{L}(A)$-estrutura.

(2) *Se existe uma imersão de* $\mathfrak{A}^*$ *em* $\mathfrak{A}'$ *como* $\mathcal{L}(A)$*-estruturas e vale* $\mathfrak{A} \prec \mathfrak{A}'$*, então* $\mathfrak{A}$ *é existencialmente fechada em* $\mathfrak{A}^*$.

Prova. (1) Para mostrar que $\mathfrak{A}^*$ pode ser imersa em $\mathfrak{A}'$ como $\mathcal{L}(A)$-estruturas, pelo Teorema 4.10.13 basta mostrar que

$$(\mathfrak{A}^*, A) \overset{\exists}{\rightsquigarrow} (\mathfrak{A}', A)$$

(a) No caso em que $\mathfrak{A}$ é existencialmente fechada em $\mathfrak{A}^*$ note que por ser $\mathsf{card}(A) \leq \mathsf{card}(A^*) < \kappa$, a estrutura $(\mathfrak{A}', A)$ é ainda κ-saturada (adicionamos menos do que κ constantes – veja a Observação 4.10.8).

Seja agora φ uma $\exists$-sentença de $\mathcal{L}(A)$ tal que

$$(\mathfrak{A}^*, A) \models \varphi.$$

Como $\mathfrak{A}$ é existencialmente fechada em $\mathfrak{A}^*$, então

$$(\mathfrak{A}, A) \models \varphi.$$

e como φ é uma $\exists$-sentença,

$$(\mathfrak{A}', A) \models \varphi.$$

(b) No caso em que cada $\mathcal{L}(A)$-subestrutura finitamente gerada de $\mathfrak{A}^*$ pode ser imersa em $\mathfrak{A}'$, afirmamos que o caso (a) também é satisfeito e portanto $\mathfrak{A}^*$ pode ser imersa em $\mathfrak{A}'$ como $\mathcal{L}(A)$-estrutura. De fato: Seja φ da forma $\exists x_1, ..., x_n\ \delta$ com δ livre de quantificadores. Se

$$(\mathfrak{A}^*, A) \models \varphi,$$

então existem elementos $a_1^*, ..., a_n^* \in A^* = |\mathfrak{A}^*|$ com

$$(\mathfrak{A}^*, A^*) \models \delta(\underline{a_1^*}, ..., \underline{a_n^*})$$

Seja $\mathfrak{B}$ a subestrutura de $\mathfrak{A}^*$ gerada por $A \cup \{a_1^*, ..., a_n^*\}$ (Por exemplo a

estrutura de interseção – veja Definição 4.9.9). Então

$$\mathfrak{A} \subset \mathfrak{B} \subset \mathfrak{A}^*$$

e, pela Definição 4.9.10, $\mathfrak{B}$ é uma $\mathcal{L}(A)$-subestrutura finitamente gerada de $\mathfrak{A}^*$. Por hipótese existe uma imersão

$$\tau : \mathfrak{B} \to \mathfrak{A}'$$

com $\tau(a) = a$ para todo $a \in A$ (identificando o domínio com sua imagem).

Pela Observação 4.7.4 e pelo Lema 4.9.3, vale então

$$(\mathfrak{A}', A) \models \delta(\underline{\tau(a_1^*)}, ..., \underline{\tau(a_n^*)}),$$

e assim, em particular

$$(\mathfrak{A}', A) \models \exists x_1, ..., x_n \; \delta.$$

(2) Se φ é uma $\mathcal{L}(A)$-sentença existencial com

$$(\mathfrak{A}^*, A) \models \varphi,$$

e existe uma imersão de $\mathfrak{A}^*$ em $\mathfrak{A}'$ como $\mathcal{L}(A)$-estruturas, então, de forma análoga à utilizada em (a), pode-se mostrar que

$$(\mathfrak{A}', A) \models \varphi.$$

Portanto, como por hipótese $\mathfrak{A} \prec \mathfrak{A}'$ obtemos

$$(\mathfrak{A}, A) \models \varphi.$$

■

O próximo corolário é consequência imediata da prova do Teorema da Imersão 4.10.13 e com o Lema do Diagrama 4.9.6 quando tomamos para $\Phi(v_0)$ não o conjunto de todas as $\exists$-fórmulas, mas sim todas as fórmulas φ da linguagem $\mathcal{L}_\gamma$ com $Fr(\varphi) \subset \{v_0\}$ e $(\mathfrak{A}, (a_\nu)_{\nu<\gamma}) \models \varphi(c_\gamma)$.

Corolário 4.10.16 *Considere as $\mathcal{L}$-estruturas $\mathfrak{A}$ e $\mathfrak{A}'$. Se $\mathfrak{A}'$ é κ-saturada, onde $\kappa \geq \mathsf{card}(|\mathfrak{A}|)$ com $\mathfrak{A}$ e $\mathfrak{A}'$ elementarmente equivalentes, então $\mathfrak{A}$ pode ser elementarmente imersa em $\mathfrak{A}'$.*

Chegamos afinal ao

Teorema 4.10.17 (Teorema do Isomorfismo) *Sejam $\mathfrak{A}$ e $\mathfrak{A}'$ duas $\mathcal{L}$-estruturas infinitas saturadas e de mesma cardinalidade κ. Então $\mathfrak{A}$ e $\mathfrak{A}'$ são isomorfas se e somente se são elementarmente equivalentes.*

Prova. Do isomorfismo entre $\mathfrak{A}$ e $\mathfrak{A}'$ segue pelo Teorema 4.7.3 imediatamente a equivalência elementar.

Para provar a recíproca, suponhamos que $\mathfrak{A}$ e $\mathfrak{A}'$ são elementarmente equivalentes. Construiremos uma indexação ordinal bijetiva $(a_\nu)_{\nu<\kappa}$ e $(a'_\nu)_{\nu<\kappa}$ de todos os elementos de $A = |\mathfrak{A}|$ e $A' = |\mathfrak{A}'|$, respectivamente, tal que valha

$$(\mathfrak{A}, (a_\nu)_{\nu<\kappa}) \equiv (\mathfrak{A}', (a'_\nu)_{\nu<\kappa}) \qquad (+)$$

na linguagem $\mathcal{L}_\kappa$ com constantes c_ν para $\nu < \kappa$ (novamente supomos sem perda de generalidade $K \cap \{\nu \mid \nu < \kappa\} = \emptyset$), o que é possível pois por hipótese $\mathfrak{A}$ e $\mathfrak{A}'$ têm a mesma cardinalidade κ.

A aplicação $\tau(a_\nu) = a'_\nu$ define, portanto, pelo Lema do Diagrama 4.9.6, uma imersão de $\mathfrak{A}$ em $\mathfrak{A}'$. Esta é obviamente sobrejetiva, ou seja, τ é um isomorfismo de $\mathfrak{A}$ em $\mathfrak{A}'$. O fato acima segue novamente como na prova do Teorema da Imersão 4.10.13, pois da validade de $(+)$ podemos concluir que $\mathfrak{A}'$ é um modelo de $D(\mathfrak{A})$.

Vamos alterar um pouco a prova do Teorema da Imersão 4.10.13 a fim de obter $(+)$.

Começamos com as indexações ordinais bijetivas $(b_\nu)_{\nu<\kappa}$ e $(b'_\nu)_{\nu<\kappa}$ de $\mathfrak{A}$ e $\mathfrak{A}'$, respectivamente. Destas indexações construímos as indexações $(a_\nu)_{\nu<\kappa}$ e $(a'_\nu)_{\nu<\kappa}$ de modo que vale

$$(\mathfrak{A}, (a_\nu)_{\nu\leq\beta}) \equiv (\mathfrak{A}', (a'_\nu)_{\nu\leq\beta}). \qquad (+)_\beta$$

para todo $\beta < \kappa$.

Disto segue imediatamente (+). De fato, a propriedade (+) segue por raciocínio análogo ao encontrado na Prova do Teorema da Imersão. Pois κ como número cardinal infinito é um número ordinal limite e cada $\mathcal{L}_\kappa$-sentença φ pode usar apenas um número finito de constantes c_ν com $\nu < \kappa$, e assim φ já é uma $\mathcal{L}_\beta$-sentença para algum $\beta < \kappa$.

Passamos a construção das sequências desejadas. Definimos as sequências $(a_\nu)_{\nu<\kappa}$ e $(a'_\nu)_{\nu<\kappa}$ tal que cada b_ν e cada b'_ν ocorram nestas sequências. Utilizamos aí o fato de que cada número ordinal γ pode ser escrito inequivocamente da forma

$$\gamma = \lambda + m,$$

onde $\lambda = 0$ ou é um número ordinal limite e $m \in \mathbb{N}$.

Seja agora $\gamma < \kappa$ e sejam as sequências (a_ν) e (a'_ν) então já definidas para $\nu < \gamma$, tal que para todo $\beta < \gamma$ a condição $(+)_\beta$ vale. Definiremos a_γ e a'_γ de modo que $(+)_\gamma$ valha. O número ordinal γ tem a representação $\gamma = \lambda + m$ como acima mencionado.

- *Caso 1* : m é par , ou seja, $m = 2n$.

Neste caso tome a_γ como aquele elemento b_ν do conjunto

$$\{b_\nu \mid \nu < \kappa\} \backslash \{a_\nu \mid \nu < \gamma\}$$

com o menor índice ν.

Para a definição de a'_γ consideramos os "Tipos de a_γ" em $(\mathfrak{A}, (a_\nu)_{\nu\leq\gamma})$, ou seja os conjuntos de fórmulas $\Phi(v_0)$ da linguagem $\mathcal{L}_\gamma$ para os quais vale

$$(\mathfrak{A}, (a_\nu)_{\nu\leq\gamma}) \models \Phi(c_\gamma).$$

Dado $\Phi(v_0)$ um tal tipo, sejam $\varphi_1, ..., \varphi_r \in \Phi(v_0)$, então vale

$$(\mathfrak{A}, (a_\nu)_{\nu<\gamma}) \models \exists v_0 \ (\varphi_1 \wedge ... \wedge \varphi_r).$$

Seja β o máximo dos índices das constantes c_ν em $(\varphi_1 \wedge ... \wedge \varphi_r) \in Fml_{\mathcal{L}_\gamma}$.

Como $\beta < \gamma$, vale $(+)_\beta$, e com isto

$$(\mathfrak{A}', (a'_\nu)_{\nu<\gamma}) \models \exists v_0 \ (\varphi_1 \wedge ... \wedge \varphi_r)$$

Assim, pelo Lema 4.10.5, $\Phi(v_0)$ é um tipo de $(\mathfrak{A}', (a'_\nu)_{\nu<\gamma})$.

Por causa da κ-saturabilidade de $\mathfrak{A}'$ e de $\mathsf{card}(\gamma) < \kappa$, existe portanto um $b'_\mu \in A'$ que realiza $\Phi(v_0)$ em $(\mathfrak{A}', |\mathfrak{A}'|)$. Seja a'_γ um tal b'_μ com o menor índice. Vale evidentemente

$$(\mathfrak{A}', (a'_\nu)_{\nu\leq\gamma}) \models \Phi(c_\gamma).$$

Note agora que se φ é uma $\mathcal{L}_{\gamma+1}$-sentença então podemos encontrar, através de uma eventual renomeação da variável vinculada, uma $\mathcal{L}_{\gamma+1}$-sentença φ' com φ e φ' logicamente equivalentes e com c_γ não estando em nenhum alcance do quantificador $\exists v_0$. Podemos assim, sem perda de generalidade, supor que $\varphi = \varphi(c_\gamma/v_0)(v_0/c_\gamma)$.

Assim, se

$$(\mathfrak{A}, (a_\nu)_{\nu\leq\gamma}) \models \varphi$$

segue portanto $\varphi(c_\gamma/v_0) \in \Phi(v_0)$, para algum tipo $\Phi(v_0)$ de $(\mathfrak{A}', (a'_\nu)_{\nu<\gamma})$. Pelo que vimos logo acima, isto implica

$$(\mathfrak{A}', (a'_\nu)_{\nu\leq\gamma}) \models \varphi.$$

Logo vale $(+)_\gamma$.

- *Caso 2* : m é ímpar, ou seja $m = 2n + 1$.

Neste caso seja a'_γ o elemento b'_ν do conjunto

$$\{b'_\nu \mid \nu < \kappa\} \backslash \{a'_\nu \mid \nu < \gamma\}$$

com o menor índice.

Definimos agora a_γ de modo totalmente analogo ao *Caso 1* e obtemos novamente

$$(\mathfrak{A}, (a_\nu)_{\nu\leq\gamma}) \equiv (\mathfrak{A}', (a'_\nu)_{\nu\leq\gamma}).$$

Do caráter alternado da definição das sequências $(a_\nu)_{\nu<\kappa}$ e $(a'_\nu)_{\nu<\kappa}$ — às vezes definimos um elemento de $(a_\nu)_{\nu<\kappa}$ a partir de elementos de $(a'_\nu)_{\nu<\kappa}$, e às vezes o contrário — concluímos agora que no *Caso 1* para o menor índice μ com $b_\mu \notin \{a_\nu \mid \nu < \gamma\}$ deve valer $\mu \geq \lambda + m$.

Analogo vale no *Caso 2* para o menor índice μ com $b'_\mu \notin \{a'_\nu \mid \nu < \gamma\}$ do mesmo modo $\mu \geq \lambda + m$. Assim finalmente atingimos todo b_μ e b'_μ.

■

4.11 Ultraprodutos

Nesta seção apresentamos uma construção algébrica que será útil para a prova do teorema principal deste texto (Teorema 5.1.7), a saber, ultraproduto de estruturas.

Ultraprodutos se assemelham a um tipo de produto módulo um certo conjunto, o qual herda propriedades semelhantes às de seus fatores, as estruturas em questão. Embora eles tenham sido introduzidos primeiramente na Teoria dos Modelos, podem ser vistos como uma construção puramente algébrica.

Para que um conjunto possa servir de "módulo" em um ultraproduto, ele precisa ter propriedades especiais, mais precisamente, precisa ser um *Ultrafiltro*. Começamos então por esta definição:

Definição 4.11.1 *Seja S um conjunto não vazio, e $P(S)$ o conjunto das partes de S. Um subconjunto não vazio $\mathcal{F}$ de $P(S)$ é chamado um filtro de S, caso*

(1) $\emptyset \notin \mathcal{F}$.

(2) $U, V \in \mathcal{F}$ *implica* $U \cap V \in \mathcal{F}$.

(3) $U \in \mathcal{F}$ *e* $U \subset A \subset S$ *implicam* $A \in \mathcal{F}$.

Como exemplos de filtros temos:

Exemplo 4.11.2 *O conjunto $\mathcal{C}$ dos subconjuntos cofinitos de S é um filtro de S:*

$$\mathcal{C} = \{A \subset S \mid S \backslash A \text{ é finito}\}.$$

Exemplo 4.11.3 *Fixado $a \in S$, o conjunto $\mathcal{H}(a) = \{A \subset S \mid a \in A\}$ é um filtro de S e tem a seguinte propriedade adicional*

(4) *$A \subset S$, $A \notin \mathcal{F}$ implica $S \backslash A \in \mathcal{F}$.*

Definição 4.11.4 *Um filtro de S que satisfaz ainda a propriedade* (4) *é dito um ultrafiltro de S. Um filtro da forma $\mathcal{H}(a)$ para algum $a \in S$, é dito um filtro principal.*

Nem todo ultrafiltro é principal: por exemplo, tomando S infinito, o filtro dos conjuntos cofinitos de S evidentemente não é principal, pois senão algum conjunto unitário pertenceria ao filtro, o que é uma contradição. Porém, pode-se provar que todo filtro de um conjunto finito necessariamente é principal.

Vale também o seguinte:

Proposição 4.11.5 *Se S é um conjunto infinito e $\mathcal{F}$ é um filtro de S que possui um conjunto finito como elemento, então $\mathcal{F}$ é um filtro principal.*

Prova. De fato, suponha $\{a_1, .., a_n\} \in \mathcal{F}$. Como S é infinito, existe $a \in S \backslash \{a_1, .., a_n\}$, de (3) segue

$$\{a_1, .., a_n, a\} \in \mathcal{F},$$

e, por (2)

$$\{a\} = \{a_1, .., a_n, a\} \cap \{a_1, .., a_n\} \in \mathcal{F}.$$

Novamente por (3)

$$\mathcal{H}(a) = \{A \subset S \mid a \in A\} \subset \mathcal{F}.$$

Por outro lado, como $\emptyset \notin \mathcal{F}$, temos que $\{a\} \cap U \neq \emptyset$ para todo $U \in \mathcal{F}$. Concluímos então que $\mathcal{F} = \mathcal{H}(a)$.

■

Sempre podemos encontrar um ultrafiltro a partir de um filtro, na verdade, o seguinte Lema nos ensina um fato mais geral ainda.

Lema 4.11.6 *Seja F_0 um conjunto de subconjuntos de S não vazio e fechado para intersecção. Então existe sempre um ultrafiltro $\mathcal{D}$ de S com $F_0 \subset \mathcal{D}$*

Prova. Seja $\mathcal{D} \subset P(S)$ uma extensão maximal de F_0 dentre todas as extensões de F_0 que não contêm o conjunto vazio e que são fechadas para intersecção. Tal elemento maximal existe pelo Lema de Zorn. Afirmamos que $\mathcal{D}$ é um ultrafiltro, o que então prova o Lema.

Consideramos o conjunto construído a partir deste conjunto maximal $\mathcal{D}$:

$$\mathcal{F}(\mathcal{D}) = \{A \subset S \mid \text{existe } U \in \mathcal{D} \text{ com } U \subset A\}.$$

Vemos que $\mathcal{F}(\mathcal{D})$ é um conjunto não vazio (pois contém $\mathcal{D}$) ainda fechado para interseção e tal que $\emptyset \notin \mathcal{F}(\mathcal{D})$ (pois nenhum conjunto não vazio está contido em $\emptyset$).

Agora é fácil verificar que $\mathcal{F}(\mathcal{D})$ é um filtro. Logo, pela maximalidade de $\mathcal{D}$, temos $\mathcal{D} = \mathcal{F}(\mathcal{D})$, e portanto $\mathcal{D}$ é um filtro de S.

Seja agora $A \subset S$ não vazio, e suponhamos que $A \notin \mathcal{D}$. Fixado $B = S \backslash A$, e construímos o conjunto

$$\mathcal{F}'(\mathcal{D}) = \mathcal{D} \cup \{U \cap B \mid U \in \mathcal{D}\}.$$

Evidentemente $\mathcal{F}'(\mathcal{D})$ é fechado para interseção. Se ocorresse $U \cap B = \emptyset$ para algum $U \in \mathcal{D}$, então teríamos $U \subset A = S \backslash B$, mas isto contradiz o fato de $A \notin \mathcal{D} = \mathcal{F}(\mathcal{D})$.

Novamente $\mathcal{F}'(\mathcal{D})$ é um filtro, e pela maximalidade de $\mathcal{D}$, o conjunto acima também deve ser igual a $\mathcal{D}$. Logo, como $S \in \mathcal{D}$, em particular

$$S \backslash A = B = S \cap B \in \mathcal{F}'(\mathcal{D}) = \mathcal{D}.$$

Com isto mostramos que $\mathcal{D}$ é um ultrafiltro de S.

■

Consideramos agora um conjunto de $\mathcal{L}$-estrutruras indexadas por um conjunto não-vazio S, digamos,

$$\{\mathfrak{A}^{(s)} \mid s \in S\}.$$

Passamos agora à construção do ultraproduto de

$$\mathfrak{A}^{(s)} = \left\langle A^{(s)}; (\mathfrak{R}_i^{(s)})_{i\in I}; (\mathfrak{f}_j^{(s)})_{j\in J}; (d_k^{(s)})_{k\in K} \right\rangle,$$

para todo $s \in S$, determinado por um ultrafiltro $\mathcal{D}$ de S que é novamente uma $\mathcal{L}$-estrutura.

Definição 4.11.7 *No conjunto de todas as sequências indexadas com* $s \in S$,

$$\prod_{s\in S} A^{(s)} = \{(a^{(s)})_{s\in S} \mid a^{(s)} \in A^{(s)} \text{ para todo } s \in S\},$$

dizemos que duas sequências $(a_1^{(s)})_{s\in S}$ *e* $(a_2^{(s)})_{s\in S}$ *são* ***equivalentes*** *quando*

$$\{s \mid a_1^{(s)} = a_2^{(s)}\} \in \mathcal{D}.$$

Quando isto ocorre, escrevemos

$$(a_1^{(s)})_{s\in S} \underset{\mathcal{D}}{\sim} (a_2^{(s)})_{s\in S},$$

ou simplesmente.

$$(a_1^{(s)})_{s\in S} \sim (a_2^{(s)})_{s\in S},$$

caso não exista chance de confusão.

Esta é de fato uma relação de equivalência em $\prod_{s\in S} A^{(s)}$, ou seja valem

(i) $(a_1^{(s)})_{s\in S} \sim (a_1^{(s)})_{s\in S}$,

(ii) $(a_1^{(s)})_{s\in S} \sim (a_2^{(s)})_{s\in S}$ implica $(a_2^{(s)})_{s\in S} \sim (a_1^{(s)})_{s\in S}$,

(iii) $(a_1^{(s)})_{s\in S} \sim (a_2^{(s)})_{s\in S}$ e $(a_2^{(s)})_{s\in S} \sim (a_3^{(s)})_{s\in S}$ implica $(a_1^{(s)})_{s\in S} \sim (a_3^{(s)})_{s\in S}$.

Por exemplo, uma vez que $\mathcal{D}$ é filtro, *(iii)* é obtida de

$$\{s \mid a_1^{(s)} = a_2^{(s)}\} \cap \{s \mid a_2^{(s)} = a_3^{(s)}\} \subset \{s \mid a_1^{(s)} = a_3^{(s)}\},$$

e portanto, por (2) e (3) da Definição 4.11.1 o conjunto maior também está em $\mathcal{D}$.

Definimos A como o conjunto quociente das classes de equivalência de $\prod_{s\in S} A^{(s)}$ pela relação $\underset{D}{\sim}$, ou seja, tomamos

$$A := \prod_{s\in S} A^{(s)}/\sim = \{\overline{(a^{(s)})} \mid (a^{(s)}) \in \prod_{s\in S} A^{(s)}\},$$

com

$$\overline{(a^{(s)})} = \{(a_1^{(s)}) \mid (a_1^{(s)}) \sim (a^{(s)})\}^9.$$

Definimos agora as relações $\mathfrak{R}_i$, as funções $\mathfrak{f}_j$ e interpretações d_k das constantes $\underline{d_k}$, de modo a tornar A o domínio da $\mathcal{L}$-estrutura

$$\mathfrak{A} = \langle A; (\mathfrak{R}_i)_{i\in I}; (\mathfrak{f}_j)_{j\in J}; (d_k)_{k\in K}\rangle .$$

Definição 4.11.8 *Sejam S um conjunto não vazio, $\mathcal{D}$ um ultrafiltro de S e $\{\mathfrak{A}^{(s)} \mid s \in S\}$ um conjunto de $\mathcal{L}$-estruturas. O <u>ultraproduto</u> de $\mathfrak{A}^{(s)}$ pelo ultrafiltro $\mathcal{D}$ é a $\mathcal{L}$-estrutura*

$$\mathfrak{A} = \langle A; (\mathfrak{R}_i)_{i\in I}; (\mathfrak{f}_j)_{j\in J}; (d_k)_{k\in K}\rangle ,$$

dada por

- $A = \prod A^{(s)}/\sim = \{\overline{(a^{(s)})} \mid (a^{(s)}) \in \prod_{s\in S} A^{(s)}\}$.
- *Para* $\overline{(a_1^{(s)})},\ldots,\overline{(a_{\lambda(i)}^{(s)})} \in A$,

$$\mathfrak{R}_i(\overline{(a_1^{(s)})}, \ldots, \overline{(a_{\lambda(i)}^{(s)})}) \text{ significa que } \{s \mid \mathfrak{R}_i^{(s)}(a_1^{(s)}, \ldots, a_{\lambda(i)}^{(s)})\} \in \mathcal{D}.$$

[9] Retiramos os subíndices ($s \in S$) para a notação ficar menos carregada. Claramente isto não causa confusão.

- *Para* $\overline{(a_1^{(s)})},...,\overline{(a_{\mu(j)}^{(s)})} \in A$,

$$\mathfrak{f}_j(\overline{(a_1^{(s)})},...,\overline{(a_{\mu(j)}^{(s)})}) := \overline{(\mathfrak{f}_j^{(s)}(a_1^{(s)},...,a_{\mu(j)}^{(s)}))}.$$

- $d_k := \overline{(d_k^{(s)})}$.

Escrevemos também

$$\mathfrak{A} = \prod_{s\in S}\mathfrak{A}^{(s)}/\mathcal{D}.$$

Precisamos verificar que as definições acima de $\mathfrak{R}_i, \mathfrak{f}_j$ e d_k independem dos representantes escolhidos.

Proposição 4.11.9 *O ultraproduto de* $\mathfrak{A}^{(s)}$ *pelo ultrafiltro* $\mathcal{D}$ *de* S *está bem definido.*

Prova. Observamos que:

- para as constantes a verificação é trivial;
- para as relações $\mathfrak{R}_i$ tomamos

$$(b_1^{(s)}) \sim (a_1^{(s)}),...,(b_{\lambda(i)}^{(s)}) \sim (a_{\lambda(i)}^{(s)}),$$

o que significa que, para todo $\nu \in \{1,...,\lambda(i)\}$,

$$\{s \mid b_\nu^{(s)} = a_\nu^{(s)}\} \in \mathcal{D},$$

e portanto

$$U = \bigcap_{1\leq\ \nu\leq\ \lambda(i)} \{s \mid b_\nu^{(s)} = a_\nu^{(s)}\} \in \mathcal{D}.$$

Assim, se vale $\mathfrak{R}_i(\overline{(a_1^{(s)})},...,\overline{(a_{\lambda(i)}^{(s)})})$, então

$$\{s \mid \mathfrak{R}_i^{(s)}(a_1^{(s)},...,a_{\lambda(i)}^{(s)})\} \in \mathcal{D},$$

e com isto

$$\{s \mid \mathfrak{R}_i^{(s)}(a_1^{(s)},...,a_{\lambda(i)}^{(s)})\} \cap U \subset \{s \mid \mathfrak{R}_i^{(s)}(b_1^{(s)},...,b_{\lambda(i)}^{(s)})\}.$$

Disto segue

$$\{s \mid \mathfrak{R}_i^{(s)}(b_1^{(s)}, ..., b_{\lambda(i)}^{(s)})\} \in \mathcal{D},$$

e então vale

$$\mathfrak{R}_i((\overline{b_1^{(s)}}), ..., (\overline{b_{\lambda(i)}^{(s)}})).$$

- para o caso das funções $\mathfrak{f}_j$ tomamos

$$(b_1^{(s)}) \sim (a_1^{(s)}), ..., (b_{\mu(j)}^{(s)}) \sim (a_{\mu(j)}^{(s)}).$$

Vale então, para todo $\nu \in \{1, ..., \mu(j)\}$,

$$\{s \mid b_\nu^{(s)} = a_\nu^{(s)}\} \in \mathcal{D},$$

e novamente

$$U = \bigcap_{1 \leq \nu \leq \mu(j)} \{s \mid b_\nu^{(s)} = a_\nu^{(s)}\} \in \mathcal{D}.$$

É óbvio que

$$U \subset \{s \mid \mathfrak{f}_j^{(s)}(a_1^{(s)}, ..., a_{\mu(j)}^{(s)}) = \mathfrak{f}_j^{(s)}(b_1^{(s)}, ..., b_{\mu(j)}^{(s)})\}.$$

Portanto obtemos

$$\{s \mid \mathfrak{f}_j^{(s)}(a_1^{(s)}, ..., a_{\mu(j)}^{(s)}) = \mathfrak{f}_j^{(s)}(b_1^{(s)}, ..., b_{\mu(j)}^{(s)})\} \in \mathcal{D}.$$

Assim, pela definição de equivalência,

$$\overline{\mathfrak{f}_j^{(s)}(a_1^{(s)}, ..., a_{\mu(j)}^{(s)})} = \overline{\mathfrak{f}_j^{(s)}(b_1^{(s)}, ..., b_{\mu(j)}^{(s)})},$$

ou ainda

$$\mathfrak{f}_j((\overline{a_1^{(s)}}), ..., (\overline{a_{\mu(j)}^{(s)}})) = \mathfrak{f}_j((\overline{b_1^{(s)}}), ..., (\overline{b_{\mu(j)}^{(s)}}))$$

■

O Teorema seguinte contém a mais importante propriedade de ultraprodutos. Para enunciá-la, precisamos do conceito de *avaliação-sequência*.

Definição 4.11.10 *Sejam*

- S *um conjunto não vazio,*
- $\mathcal{D}$ *um ultrafiltro de* S*,*
- $\{\mathfrak{A}^{(s)} \mid s \in S\}$ *um conjunto de* $\mathcal{L}$*-estruturas,*
- $\mathfrak{A} = \prod_{s \in S} \mathfrak{A}^{(s)}/\mathcal{D}$ *o ultraproduto de* $\mathfrak{A}^{(s)}$ *pelo ultrafiltro* $\mathcal{D}$*,*
- $A = |\mathfrak{A}|$*,*
- $h^{(s)}$*, uma avaliação em* $\mathfrak{A}^{(s)}$ *para cada* $s \in S$*.*

Então definimos a avaliação-sequência em $\mathfrak{A}$ *, determinada pelas* $h^{(s)}$*, como a aplicação*

$$(\overline{h^{(s)}}) : Vbl \longrightarrow A,$$

através de $(\overline{h^{(s)}})(v) := (\overline{h^{(s)}(v)})$*, que é obviamente uma avaliação em* $\mathfrak{A}$*.*

Observação 4.11.11 *Dado* $a = (\overline{a^{(s)}})$ *um elemento de* $A = \prod A^{(s)}/\sim$*, salientamos que*

$$(\overline{h^{(s)}})(x, a) = (\overline{h^{(s)}(x, a^{(s)})}).$$

De fato, pela Definição 4.4.3, para cada $v \in Vbl$ *vale*

$$(\overline{h^{(s)}})(x, a)(v) = \begin{cases} (\overline{h^{(s)}})(v) = (\overline{h^{(s)}(v)}), & \text{se } v \neq x, \\ a = (\overline{a^{(s)}}), & \text{se } v = x. \end{cases}$$

Teorema 4.11.12 (Teorema de Los) *Seja* $\mathfrak{A}$ *o Ultraproduto de* $\mathcal{L}$*-estruturas* $\mathfrak{A}^{(s)}$ *com* $s \in S$ *por um Ultrafiltro* $\mathcal{D}$ *de* S*. Então, para cada* $\mathcal{L}$*-fórmula* φ *e cada avaliação-sequencia* $(\overline{h^{(s)}})$ *em* $\mathfrak{A}$

$$\mathfrak{A} \models \varphi[(\overline{h^{(s)}})] \text{ se e só se } \{s \mid \mathfrak{A}^{(s)} \models \varphi[h^{(s)}]\} \in \mathcal{D}.$$

Prova. Provamos esta equivalência por indução sobre a construção de φ.

- Se φ é uma fórmula atômica, então a equivalência do Teorema resulta da definição de igualdade de classes de equivalência assim como da definição

da relação $\mathfrak{R}_i$ para cada $i \in I$. Basta para isto observar a identidade

$$t^{\mathfrak{A}}[(\overline{h^{(s)}})] = (\overline{t^{\mathfrak{A}^{(s)}}[h^{(s)}]}),$$

o que se prova a partir da construção de termos de maneira rotineira .

- Se φ é da forma $\neg\varphi_1$, então, pela hipótese de indução e pela propriedade (4) de Ultrafiltros,

$$\begin{aligned}
\mathfrak{A} \models \neg\varphi_1[(\overline{h^{(s)}})] \quad &\Leftrightarrow \quad \mathfrak{A} \not\models \varphi_1[(\overline{h^{(s)}} \\
&\overset{\text{Hip. Ind.}}{\Leftrightarrow} \quad \{s \mid \mathfrak{A}^{(s)} \models \varphi_1[h^{(s)}]\} \notin \mathcal{D} \\
&\overset{\text{Propri. (4)}}{\Leftrightarrow} \quad S\backslash\{s \mid \mathfrak{A}^{(s)} \models \varphi_1[h^{(s)}]\} \in \mathcal{D} \\
&\Leftrightarrow \quad \{s \mid \mathfrak{A}^{(s)} \not\models \varphi_1[h^{(s)}]\} \in \mathcal{D} \\
&\Leftrightarrow \quad \{s \mid \mathfrak{A}^{(s)} \models \neg\varphi_1[h^{(s)}]\} \in \mathcal{D}.
\end{aligned}$$

- Se φ é da forma $(\varphi_1 \wedge \varphi_2)$, então temos, pela hipótese de indução e pelas propriedades (2) e (3) de ultrafiltros,

$$\begin{aligned}
\mathfrak{A} \models \varphi[(\overline{h^{(s)}})] \quad &\Leftrightarrow \quad (\mathfrak{A} \models \varphi_1[\overline{h^{(s)}}] \text{ e } \mathfrak{A} \models \varphi_2[\overline{h^{(s)}}]) \\
&\overset{\text{Hip. Ind.}}{\Leftrightarrow} \quad (\{s \mid \mathfrak{A}^{(s)} \models \varphi_1[h^{(s)}]\} \in \mathcal{D} \\
&\qquad \text{e } \{s \mid \mathcal{A}^{(s)} \models \varphi_2[h^{(s)}]\} \in \mathcal{D}) \\
&\overset{\text{Propri. (2) e (3)}}{\Leftrightarrow} \quad \{s \mid \mathfrak{A}^{(s)} \models \varphi_1[h^{(s)}]\} \\
&\qquad \cap \{s \mid \mathfrak{A}^{(s)} \models \varphi_2[h^{(s)}]\} \in \mathcal{D} \\
&\Leftrightarrow \quad \{s \mid \mathfrak{A}^{(s)} \models (\varphi_1 \wedge \varphi_2)[h^{(s)}]\} \in \mathcal{D}.
\end{aligned}$$

Aí utilizamos com a hipótese de indução as propriedades (2) e (3) de filtros.

- Se φ é da forma $\forall x\ \varphi_1$, então

$$\begin{aligned}
\mathfrak{A} \models \varphi[(\overline{h^{(s)}})] \quad &\Leftrightarrow \quad \mathfrak{A} \models \varphi_1[(\overline{h^{(s)}})(x, a)] \text{ para todo } a \in A \\
&\overset{\text{Obs. 4.11.11}}{\Leftrightarrow} \quad \mathfrak{A} \models \varphi_1[(\overline{h^{(s)}(x, a^{(s)})})] \text{ para todo } (a^{(s)}) \in \prod_{s \in S} A^{(s)} \\
&\Leftrightarrow \quad \{s \mid \mathfrak{A}^{(s)} \models \varphi_1[h^{(s)}(x, a^{(s)})]\} \in \mathcal{D} \\
&\qquad \text{para todo } (a^{(s)}) \in \prod_{s \in S} A^{(s)}
\end{aligned}$$

$$\begin{aligned} &\Leftrightarrow \{s \mid \mathfrak{A}^{(s)} \models \varphi_1[h^{(s)}(x, a^{(s)})] \\ &\qquad \text{para todo } a^{(s)} \in A^{(s)}\} \in \mathcal{D} \\ &\Leftrightarrow \{s \mid \mathfrak{A}^{(s)} \models \forall x\, \varphi_1[h^{(s)}]\} \in \mathcal{D}. \end{aligned}$$

Mas a penúltima equivalência precisa ainda ser mostrada. Fixamos para isto

$$U = \{s \mid \mathfrak{A}^{(s)} \models \varphi_1[h^{(s)}(x, a^{(s)})] \text{ para todo } a^{(s)} \in A^{(s)}\}.$$

Para cada sequência $(b^{(s)}) \in \prod_{s \in S} A^{(s)}$ vale então

$$U \subset \{s \mid \mathfrak{A}^{(s)} \models \varphi_1[h^{(s)}(x, b^{(s)})]\}.$$

Com isto segue a direção ($\Leftarrow$) pela propriedade (3) de filtros. Falta provar ($\Rightarrow$). Supomos $U \notin \mathcal{D}$. Segue que $S \backslash U \in \mathcal{D}$, e disto

$$V = \{s \mid \mathfrak{A}^{(s)} \not\models \varphi_1[h^{(s)}(x, a^{(s)})] \text{ para algum } a^{(s)} \in A^{(s)}\} \in \mathcal{D}.$$

Definimos agora uma sequência $(b^{(s)})$ através de

$$b^{(s)} = \begin{cases} \text{um } a^{(s)} \text{ com } \mathfrak{A}^{(s)} \not\models \varphi_1[h^{(s)}(x, a^{(s)})], \text{ caso } s \in V; \\ \text{um } a^{(s)} \in A^{(s)}, \text{ caso contrário.} \end{cases}$$

Vale então

$$V \subset \{s \mid \mathfrak{A}^{(s)} \not\models \varphi_1[h^{(s)}(x, b^{(s)})]\}.$$

Como $V \in \mathcal{D}$, o conjunto acima à direita pertence também ao conjunto $\mathcal{D}$, e com isto, por (1) e por (2) da Definição 4.11.1

$$\{s \mid \mathfrak{A}^{(s)} \models \varphi_1[h^{(s)}(x, b^{(s)})]\} \notin \mathcal{D}.$$

Isto porém contradiz a hipótese.

■

Consideramos agora o caso especial em que todas as estruturas $\mathfrak{A}^{(s)}$ são iguais, a saber $\mathfrak{A}^{(s)} = \mathfrak{A}$ para todo $s \in S$. Neste caso dizemos que

Definição 4.11.13 *Sejam $\mathfrak{A}$ uma $\mathcal{L}$-estrutura, S um conjunto não vazio e $\mathcal{D}$ um ultrafiltro de $\mathcal{D}$. O ultraproduto*

$$\mathfrak{A}^S/\mathcal{D} := \mathfrak{A}^* = \prod_{s\in S}\mathfrak{A}/\mathcal{D}.$$

é chamado também de ultrapotência de $\mathfrak{A}$ por $\mathcal{D}$.

Corolário 4.11.14 *Sejam $\mathfrak{A}$ uma $\mathcal{L}$-estrutura e $\mathcal{D}$ um ultrafiltro de S. Então a aplicação*

$$\tau : \mathfrak{A} \to \mathfrak{A}^*$$

dada por $\tau(b) = (\overline{b})_{s\in S}$, para todo $b \in |\mathfrak{A}|$, define uma imersão elementar de $\mathfrak{A}$ na ultrapotência $\mathfrak{A}^* = \mathfrak{A}^S/\mathcal{D}$.

Prova. Seja h uma avaliação em $\mathfrak{A}$. A partir de h construímos a avaliação sequência $\overline{h}$ na ultrapotência $\mathfrak{A}^*$

$$\overline{h}(x) = (\overline{h(x)})_{s\in S} = \tau(h(x)).$$

Para cada $\mathcal{L}$-fórmula φ e cada avaliação h em $\mathfrak{A}$ vale então pelo Teorema 4.11.12

$$\mathfrak{A}^* \models \varphi[\overline{h}] \text{ se e só se } \{s \mid \mathfrak{A} \models \varphi[h]\} \in \mathcal{D}.$$

Como a condição $\mathfrak{A} \models \varphi[h]$ não depende de s, o conjunto $\{s \mid \mathfrak{A} \models \varphi[h]\}$ só pode ser o conjunto vazio ou o conjunto S. Como $\emptyset \notin \mathcal{D}$ e $S \in \mathcal{D}$ obtemos

$$\{s \mid \mathfrak{A} \models \varphi[h]\} \in \mathcal{D} \text{ se e só se } \mathfrak{A} \models \varphi[h].$$

Em suma temos

$$\mathfrak{A} \models \varphi[h] \text{ se e só se } \mathfrak{A}^* \models \varphi[\tau \circ h].$$

Isto significa que τ é um imersão elementar de $\mathfrak{A}$ em $\mathfrak{A}^*$

■

Corolário 4.11.15 *Como τ é uma imersão elementar de $\mathfrak{A}$ em $\mathfrak{A}^*$, em particular provamos que*

$$\mathfrak{A} \equiv \mathfrak{A}^S/\mathcal{D}.$$

Com ultrapotências em mãos temos outro método para construir extensões elementares de estruturas.

Como aplicação de ultraprodutos damos uma outra prova para o Teorema da Finitude (Teorema 4.4.15) que não faz uso do Teorema da Completude de Gödel (Teorema 4.4.10).

Dado um conjunto Σ de $\mathcal{L}$-sentenças, denotamos por S o conjunto de todos os subconjuntos finitos Δ de Σ. O conjunto S é parcialmente ordenado com relação à inclusão de conjuntos. Além disso, seja F_0 o conjunto de todos os conjuntos não vazios da forma

$$S_\Delta = \{\Delta' \in S \mid \Delta \subset \Delta'\},$$

onde Δ percorre todos os elementos de S. F_0 é fechado para interseção, pois

$$S_{\Delta_1} \cap S_{\Delta_2} = S_{\Delta_1 \cup \Delta_2}.$$

Pelo Lema 4.11.6 existe um ultrafiltro $\mathcal{D}$ de S, que contém F_0. Vale então

Teorema 4.11.16 *Seja Σ um conjunto de $\mathcal{L}$-sentenças tal que todo subconjunto finito Δ possui um modelo. Seja S o conjunto de todos os subconjuntos finitos Δ de Σ. Tome $\mathcal{D}$ um ultrafiltro de S que contém o conjunto F_0 construído acima. Para cada $\Delta \in S$ seja $\mathfrak{A}^{(\Delta)}$ um modelo de Δ. Então o Ultraproduto*

$$\mathfrak{A} = \prod_{\Delta \in S} \mathfrak{A}^{(\Delta)}/\mathcal{D}$$

é um modelo de Σ.

Prova. Seja $\rho \in \Sigma$. Para cada $\Delta \in S$ com $\rho \in \Delta$ vale evidentemente $\mathfrak{A}^{(\Delta)} \models \rho$. Vale ainda

$$\{\Delta \mid \mathfrak{A}^{(\Delta)} \models \rho\} \supset \{\Delta \mid \Delta \supset \{\rho\}\} = S_{\{\rho\}}.$$

Como $S_{\{\rho\}} \in F_0 \subset \mathcal{D}$ segue que

$$\{\Delta \mid \mathfrak{A}^{(\Delta)} \models \rho\} \in \mathcal{D}.$$

o Teorema de Los 4.11.12 temos então

$$\mathfrak{A} \models \rho.$$

Portanto

$$\mathfrak{A} \models \Sigma$$

■

4.12 Propriedades da classe dos modelos

Nesta seção definimos a classe de modelos de um fixado sistema de axiomas Σ de uma linguagem $\mathcal{L}$, também fixada, e estudamos suas propriedades.

Primeiramente equipamos tal classe com uma topologia que a torna um espaço compacto. Esta propriedade é precisamente o conteúdo do Teorema da Finitude (Teorema 4.4.15). Depois disto, introduzimos mais propriedades de Σ e, respectivamente da sua classe de modelos, a saber: compacidade, separação, completude e modelo-completude. O estudo destas propriedades não é feito apenas para fins de uma possível aplicação na prova da completude de uma Teoria, mas também por serem ferramentas úteis na matemática, em especial nas teorias algébricas.

4.12.1 Compacidade e Separação

Definição 4.12.1 *Fixamos uma linguagem $\mathcal{L} = (\lambda, \mu, K)$ e denotamos por $Mod_{\mathcal{L}}$ a classe de todas as $\mathcal{L}$-estruturas $\mathfrak{A}$. Dado um subconjunto Σ de $Sent_{\mathcal{L}}$ definimos a classe de (todos os) modelos de Σ: como sendo a classe*

$$Mod_{\mathcal{L}}(\Sigma) = \{\mathfrak{A} \in Mod_{\mathcal{L}} \mid \mathfrak{A} \models \Sigma\}.$$

Notação 4.12.2 *Para $\Sigma = \{\sigma\}$ escrevemos no lugar de $Mod_{\mathcal{L}}(\{\sigma\})$ resumidamente $Mod_{\mathcal{L}}(\sigma)$.*

Também no que segue, esqueceremos o índice $\mathcal{L}$ sempre que estiver claro de qual linguagem $\mathcal{L}$ estamos tratatando.

Lema 4.12.3 *Com as notações acima introduzidas, temos:*

i) $Mod(\exists x\ x \neq x) = \emptyset$

ii) $Mod(\forall x\ x \doteq x) = Mod$

iii) $Mod(\neg\varphi) = Mod \backslash Mod(\varphi)$

iv) $Mod(\varphi \wedge \psi) = Mod(\varphi) \cap Mod(\psi)$

v) $Mod(\varphi \vee \psi) = Mod(\varphi) \cup Mod(\psi)$

vi) $Mod(\Sigma) = \bigcap_{\sigma \in \Sigma} Mod(\sigma)$

Prova. Imediata.

■

A classe $\{Mod(\varphi) \mid \varphi \in Sent_{\mathcal{L}}\}$ é fechada para intersecção (por (iv)) e pode por isto servir como uma base de uma topologia para Mod. Dizemos assim que uma subclasse de Mod é um aberto, quando é simplesmente uma união de classes da forma $Mod(\varphi)$ com $\varphi \in Sent_{\mathcal{L}}$, ou seja, os conjuntos abertos nesta topologia são da forma

$$\bigcup_{\varphi \in \Phi} Mod(\varphi),$$

onde Φ é um subconjunto de $Sent_{\mathcal{L}}$. As classes fechadas são os complementares de abertos, e por (iii), são da forma

$$\bigcap_{\varphi \in \Phi} Mod(\neg\varphi),$$

ou seja, são precisamente classes de modelos como introduzimos acima (fixe $\Sigma = \{\neg\varphi \mid \varphi \in \Phi\}$).

Definição 4.12.4 *Um subconjunto fechado de $Mod_{\mathcal{L}}$ é dito elementar ou axiomatizável.*

Observação 4.12.5 *Podemos notar ainda que, no sentido de Teoria dos Conjuntos, $Mod_{\mathcal{L}}$ é uma classe própria . Assim, a introdução de uma topologia sobre $Mod_{\mathcal{L}}$ pode parecer um pouco suspeita. Porém, não nos importaremos com tal ponto, pois por procedimentos precisos de Teoria dos Conjuntos este defeito pode ser remediado: pode-se por exemplo, limitar $Mod_{\mathcal{L}}$ àquelas estruturas pertencentes a um conjunto V pré-fixado . Com isto, escolhemos o 'universo' V tão grande que todas as operações interessantes de conjuntos lá podem ser feitas.*

Como primeira observação sobre esta topologia, notamos que Mod é um espaço não Hausdorff. Esta propriedade pode ser constatada da seguinte reformulação de equivalência elementar de $\mathcal{L}$-estruturas $\mathfrak{A}$ e $\mathfrak{B}$:

$$\mathfrak{A} \in Mod(\sigma) \text{ se e só se } \mathfrak{B} \in Mod(\sigma)$$

para todo $\sigma \in Sent_{\mathcal{L}}$. Assim, se $\mathfrak{A} \equiv \mathfrak{B}$ e $\mathfrak{A}$ pertence a um aberto $Mod(\sigma)$, então também $\mathfrak{B}$ pertence a este aberto, logo $\mathfrak{A}$ não poderá ser "separado" de $\mathfrak{B}$, mesmo sendo ambas estruturas distintas.

Reinterpretaramos a seguir o Teorema da Finitude (Teorema 4.4.15), enunciando-o como a compacidade do espaço $Mod_{\mathcal{L}}(\Sigma)$. Esta tradução não é difícil, contudo muito relevante.

Teorema 4.12.6 (Teorema da Compacidade) *Seja $\Sigma \subset Sent_{\mathcal{L}}$. Então $Mod_{\mathcal{L}}(\Sigma)$ tem a propriedade de 'Heine-Borel', ou seja, se $\bigcup_{\varphi \in \Phi} Mod_{\mathcal{L}}(\varphi)$ é uma cobertura por abertos de $Mod_{\mathcal{L}}(\Sigma)$, então existem $\varphi_1, ...\varphi_n \in \Phi$ tais que*

$$Mod_{\mathcal{L}}(\Sigma) \subset Mod_{\mathcal{L}}(\varphi_1) \cup ... \cup Mod_{\mathcal{L}}(\varphi_n).$$

Prova. Da hipótese e pela propriedade (vi) do Lema 4.12.3,

$$Mod_{\mathcal{L}}(\Sigma) = \bigcap_{\sigma \in \Sigma} Mod(\sigma) \subset \bigcup_{\varphi \in \Phi} Mod(\varphi)$$

e segue imediatamente

$$\bigcap_{\sigma\in\Sigma} Mod(\sigma) \cap \bigcap_{\varphi\in\Phi} Mod(\neg\varphi) = \emptyset,$$

ou seja, o conjunto $\Sigma \cup \{\neg\varphi \mid \varphi \in \Phi\}$ não possui nenhum modelo. Portanto, pelo Teorema 4.4.15, existe um subconjunto finito de $\Sigma \cup \{\neg\varphi \mid \varphi \in \Phi\}$ que possui nenhum modelo, ou seja, existe um conjunto $\{\varphi_1, ..., \varphi_n\} \subset \Phi$, tal que

$$Mod(\Sigma) \cap Mod(\neg\varphi_1) \cap ... \cap Mod(\neg\varphi_n) = \emptyset$$

Mas isto significa precisamente

$$Mod(\Sigma) \subset Mod(\varphi_1) \cup ... \cup Mod(\varphi_n),$$

o que completa a prova.

■

O Teorema da Compacidade também implica o Teorema da Finitude. De fato, caso $\Sigma \subset Sent_{\mathcal{L}}$ não possua nenhum modelo, então

$$\bigcap_{\sigma\in\Sigma} Mod(\sigma) = \emptyset,$$

e pelo Lema 4.12.3, o complementar

$$\bigcup_{\sigma\in\Sigma} Mod(\neg\sigma)$$

é uma cobertura do complementar de Φ, ou seja, de Mod. Pelo Teorema da Compacidade existem $\sigma_1, ..., \sigma_n \in \Sigma$, tais que $Mod(\neg\sigma_1) \cup ... \cup Mod(\neg\sigma_n)$ já cobre Mod. Assim,

$$Mod(\sigma_1) \cap ... \cap Mod(\sigma_n) = \emptyset,$$

ou seja, o subconjunto finito $\{\sigma_1, ..., \sigma_n\}$ de Σ não possui nenhum modelo.

Do Teorema da Compacidade deduzimos também o chamado Lema da Separação.

Lema 4.12.7 (Lema da Separação) *Sejam* $\Sigma_1, \Sigma_2, \Gamma \subset Sent_{\mathcal{L}}$ *com*

$$Mod_{\mathcal{L}}(\Sigma_i) \neq \emptyset$$

para $i = 1, 2$. *Se, para cada par fixado* $\mathfrak{A} \in Mod_{\mathcal{L}}(\Sigma_1)$ *e* $\mathfrak{B} \in Mod_{\mathcal{L}}(\Sigma_2)$, *existe um* $\gamma \in \Gamma$ *com*

$$\mathfrak{A} \models \gamma \quad e \quad \mathfrak{B} \models \neg\gamma,$$

então existe um γ^* *com*

$$Mod_{\mathcal{L}}(\Sigma_1) \subset Mod_{\mathcal{L}}(\gamma^*) \ \ e \ \ Mod_{\mathcal{L}}(\Sigma_2) \subset Mod_{\mathcal{L}}(\neg\gamma^*).$$

Tal γ^* *pode ser tomado como uma disjunção finita de conjunções finitas de elementos de* Γ.

Prova. Fixamos primeiramente um modelo $\mathfrak{A} \in Mod(\Sigma_1)$ e escolhemos para cada $\mathfrak{B} \in Mod(\Sigma_2)$ um $\gamma_{\mathfrak{B}}$ que satisfaz

$$\mathfrak{A} \in Mod(\gamma_{\mathfrak{B}}) \quad \text{e} \quad \mathfrak{B} \in Mod(\neg\gamma_{\mathfrak{B}}),$$

cuja existência é garantida pela hipótese. Portanto, evidentemente, as classes $Mod(\neg\gamma_{\mathfrak{B}})$ formam uma cobertura aberta de $Mod(\Sigma_2)$. Pelo Teorema da Compacidade (Teorema 4.12.6) existem $\mathfrak{B}_1, ..., \mathfrak{B}_m \in Mod(\Sigma_2)$, tais que

$$Mod(\Sigma_2) \subset Mod(\neg\gamma_{\mathfrak{B}_1}) \cup ... \cup Mod(\neg\gamma_{\mathfrak{B}_m}) \overset{\text{Lema 4.12.3}}{=} Mod(\neg(\gamma_{\mathfrak{B}_1} \wedge ... \wedge \gamma_{\mathfrak{B}_m})).$$

Definindo então

$$\gamma_{\mathfrak{A}} = (\gamma_{\mathfrak{B}_1} \wedge ... \wedge \gamma_{\mathfrak{B}_m}),$$

temos

$$\mathfrak{A} \in Mod(\gamma_{\mathfrak{A}}) \quad \text{e} \quad Mod(\Sigma_2) \subset Mod(\neg\gamma_{\mathfrak{A}}). \tag{97}$$

Por outro lado, evidentemente, como $\mathfrak{A} \in Mod(\gamma_{\mathfrak{A}})$, as classes $Mod(\gamma_{\mathfrak{A}})$ cobrem a classe $Mod(\Sigma_1)$. Novamente, pelo Teorema da Compacidade,

existem $\mathfrak{A}_1, ..., \mathfrak{A}_n \in Mod(\Sigma_1)$, tais que

$$Mod(\Sigma_1) \subset Mod(\gamma_{\mathfrak{A}_1}) \cup ... \cup Mod(\gamma_{\mathfrak{A}_n}) \overset{\text{Lema 4.12.3}}{=} Mod(\gamma_{\mathfrak{A}_1} \vee ... \vee \gamma_{\mathfrak{A}_n}).$$

Como por (97) vale também

$$Mod(\Sigma_2) \subset Mod(\neg\gamma_{\mathfrak{A}_1}) \cap ... \cap Mod(\neg\gamma_{\mathfrak{A}_n}) = Mod(\neg(\gamma_{\mathfrak{A}_1} \vee ... \vee \gamma_{\mathfrak{A}_n})),$$

definimos finalmente

$$\gamma^* = (\gamma_{\mathfrak{A}_1} \vee ... \vee \gamma_{\mathfrak{A}_n}),$$

que tem a propriedade desejada.

■

O próximo Lema é uma consequência do Lema da Separação mais confortável para aplicações. Antes generalizamos a maneira de escrita utilizada no Teorema 4.10.13.

Definição 4.12.8 *Dadas $\mathcal{L}$-estruturas $\mathfrak{A}$, $\mathfrak{B}$ e $\Gamma \subset Sent_{\mathcal{L}}$ escrevemos*

$$\mathfrak{A} \overset{\Gamma}{\rightsquigarrow} \mathfrak{B}$$

para significar que, para todo $\gamma \in \Gamma$ vale:

$$\mathfrak{A} \models \gamma \quad \textit{implica} \quad \mathfrak{B} \models \gamma.$$

Notação 4.12.9 *Para $\mathfrak{A} \overset{\{\gamma\}}{\rightsquigarrow} \mathfrak{B}$ escrevemos resumidamente $\mathfrak{A} \overset{\gamma}{\rightsquigarrow} \mathfrak{B}$.*

Lema 4.12.10 *Sejam $\Sigma, \Gamma, \{\varphi\} \subset Sent_{\mathcal{L}}$ e sejam γ_0 um elemento de Γ que não vale em nenhum modelo de Σ e γ_1 um elemento de Γ que vale em todo modelo de Σ.*

Se, para todos os modelos $\mathfrak{A}$ e $\mathfrak{B}$ de Σ vale

$$(\mathfrak{A} \overset{\Gamma}{\rightsquigarrow} \mathfrak{B} \;\Rightarrow\; \mathfrak{A} \overset{\varphi}{\rightsquigarrow} \mathfrak{B}),$$

então existe uma disjunção finita γ^* de conjunções finitas de elementos de

Γ , *a qual é equivalente a* φ *em todo modelo de* Σ, *ou seja,*

$$\Sigma \vdash (\varphi \leftrightarrow \gamma^*).$$

Prova. Colocamos no Lema da Separação $\Sigma_1 = \Sigma \cup \{\varphi\}$ e $\Sigma_2 = \Sigma \cup \{\neg\varphi\}$.

- Se $Mod(\Sigma_1) = \emptyset$, então vale evidentemente, pelo Teorema da Completude (Teorema 4.4.10)

$$\Sigma \vdash (\varphi \leftrightarrow \gamma_0);$$

- Se $Mod(\Sigma_2) = \emptyset$ então vale analogamente $\Sigma \vdash (\varphi \leftrightarrow \gamma_1)$.

- Sejam agora $\mathfrak{A} \in Mod(\Sigma_1)$ e $\mathfrak{B} \in Mod(\Sigma_2)$, então por hipótese, se não vale $\mathfrak{A} \overset{\varphi}{\rightsquigarrow} \mathfrak{B}$, também não vale $\mathfrak{A} \overset{\Gamma}{\rightsquigarrow} \mathfrak{B}$. Logo, existe um $\gamma \in \Gamma$ com

$$\mathfrak{A} \models \gamma \quad \text{e} \quad \mathfrak{B} \models \neg\gamma.$$

Pelo Lema da Separação, obtemos uma disjunção finita γ^* de finitas conjunções de elementos de Γ com $Mod(\Sigma_1) \subset Mod(\gamma^*)$ e $Mod(\Sigma_2) \subset Mod(\neg\gamma^*)$. Daqui obtém-se que, para $\mathfrak{A} \in Mod(\Sigma)$, por um lado

$$\mathfrak{A} \models \varphi \text{ implica } \mathfrak{A} \models \gamma^*$$

e, por outro lado,

$$\mathfrak{A} \models \neg\varphi \text{ implica } \mathfrak{A} \models \neg\gamma^*.$$

Assim temos para todo $\mathfrak{A} \in Mod(\Sigma)$ também

$$\mathfrak{A} \models (\varphi \leftrightarrow \gamma^*)$$

Pelo Teorema da Completude de Gödel (Teorema 4.4.10) segue então

$$\Sigma \vdash (\varphi \leftrightarrow \gamma^*).$$

■

Como uma aplicação do Lema 4.12.10 obtemos

Teorema 4.12.11 *Sejam* $\Sigma, \{\varphi\} \subset Sent_{\mathcal{L}}$. *Se para todo* $\mathfrak{B}, \mathfrak{B}_1 \in Mod(\Sigma)$

com $\mathfrak{B} \subset \mathfrak{B}_1$ *vale*

$$\mathfrak{B}_1 \overset{\varphi}{\rightsquigarrow} \mathfrak{B},$$

então existe uma $\mathcal{L}$*-fórmula* δ *, livre de quantificadores, com* $\Sigma \vdash (\varphi \leftrightarrow \forall\delta)$*. (Aqui* $\forall\delta$ *é uma sentença.)*

Prova. Inicialmente definimos

$$\Gamma = \{\forall\delta \mid \delta \in Fml_{\mathcal{L}} \text{ e } \delta \text{ é livre de quantificadores}\} \subset Sent_{\mathcal{L}},$$

e mostramos que para todo $\mathfrak{A}, \mathfrak{B} \in Mod(\Sigma)$, se valer $\mathfrak{A} \overset{\Gamma}{\rightsquigarrow} \mathfrak{B}$, então vale também $\mathfrak{A} \overset{\varphi}{\rightsquigarrow} \mathfrak{B}$, pois daí poderemos aplicar o lema anterior.

Com este intuito, observamos que a hipótese $\mathfrak{A} \overset{\Gamma}{\rightsquigarrow} \mathfrak{B}$, se lida como a sua contrapositiva, diz que toda $\exists$-sentença que vale em $\mathfrak{B}$, também já valia em $\mathfrak{A}$.

Com o Teorema da Existência 4.10.9 conseguimos uma κ^+-saturada (e portanto κ-saturada) extensão elementar $\mathfrak{A}'$ de $\mathfrak{A}$, onde escolhemos $\kappa \geq \mathsf{card}(|\mathfrak{B}|)$. Em particular, por ser elementarmente equivalente a $\mathfrak{A}$, temos que $\mathfrak{A}'$ é também um modelo de Σ. Pelo Teorema da Imersão 4.10.13 a estrutura $\mathfrak{B}$ pode ser imersa em $\mathfrak{A}'$. Pela hipótese do Teorema:

$$\mathfrak{A}' \models \varphi \quad \text{implica} \quad \mathfrak{B} \models \varphi.$$

Como $\mathfrak{A} \equiv \mathfrak{A}'$, segue que

$$\mathfrak{A} \overset{\varphi}{\rightsquigarrow} \mathfrak{B}$$

Para podermos aplicar o Lema 4.12.10, observamos ainda que podemos tomar como γ_0 a sentença $(\forall\, v_0\ v_0 \neq v_0)$, e como γ_1, a sentença $(\forall\, v_0\ v_0 \doteq v_0)$.

Com o Lema 4.12.10, segue que

$$\Sigma \vdash (\varphi \leftrightarrow \gamma^*),$$

onde γ^* é uma disjunção finita de conjunções finitas de Γ.

É fácil se convencer agora, por um argumento puramente lógico, pela

escolha acima de Γ, que γ^*é equivalente a uma $\gamma \in \Gamma$.[10] Assim, $(\gamma^* \leftrightarrow \gamma)$ é uma tautologia, e portanto $\Sigma \vdash (\gamma^* \leftrightarrow \gamma)$. Com isto o teorema fica provado.

■

4.12.2 Completude

Aqui o objetivo é apresentar dois resultados importantes do ponto de vista teórico, e realmente de fácil verificação.

Na Seção 4.5 um sistema de axiomas $\Sigma \subset Sent_{\mathcal{L}}$, não contraditório foi chamado completo quando para cada $\sigma \in Sent_{\mathcal{L}}$ vale

$$\Sigma \vdash \sigma \quad \text{ou} \quad \Sigma \vdash \neg\sigma.$$

Para uma $\mathcal{L}$-teoria T isto significa que (veja Definição 4.5.9)

$$\sigma \in T \quad \text{ou} \quad \neg\sigma \in T.$$

Também vimos que as $\mathcal{L}$-teorias completas T sempre são da forma $Th(\mathfrak{A})$ para alguma $\mathcal{L}$-estrutura $\mathfrak{A}$ (veja comentários abaixo da Definição 4.5.9).

Um outro critério trivial é

Lema 4.12.12 *$\Sigma \subset Sent_{\mathcal{L}}$ é completo $\Leftrightarrow$ quaisquer dois modelos de Σ são elementarmente equivalentes.*

Prova. Se Σ é completo, então

$$Ded(\Sigma) = Th(\mathfrak{A})$$

para alguma $\mathcal{L}$-estrutura $\mathfrak{A}$. Se $\mathfrak{B}$ é um modelo de Σ então vale naturalmente

$$\mathfrak{B} \models Th(\mathfrak{A})$$

pelo Teorema 4.4.13. Daí segue imediatamente $\mathfrak{A} \equiv \mathfrak{B}$.

[10] $(\forall\delta_1 \wedge \forall\delta_2 \leftrightarrow \forall(\delta_1 \wedge \delta_2))$ e $(\forall\delta_1 \vee \forall\delta_2 \leftrightarrow \forall(\delta_1 \vee \delta_2))$

Seja $\mathfrak{C}$ um outro modelo de Σ, então segue analogamente

$$\mathfrak{A} \equiv \mathfrak{C},$$

e em particular

$$\mathfrak{B} \equiv \mathfrak{C}.$$

Se Σ não é completo, então existe uma $\sigma \in Sent_{\mathcal{L}}$ com

$$\Sigma \nvdash \sigma \quad \text{e} \quad \Sigma \nvdash \neg\sigma.$$

Pelo Teorema da Completude de Gödel, existem então modelos $\mathfrak{A}$ e $\mathfrak{B}$ de Σ com

$$\mathfrak{A} \models \neg\sigma \quad \text{e} \quad \mathfrak{B} \models \sigma.$$

e portanto não vale $\mathfrak{A} \equiv \mathfrak{B}$. Com isto mostramos a equivalência.

■

Um outro critério suficiente para a completude.

Teorema 4.12.13 (Teste de Vaught) *Se um conjunto $\Sigma \subset Sent_{\mathcal{L}}$ possui apenas modelos infinitos e existe um número cardinal $\kappa \geq \kappa_{\mathcal{L}}$, tal que quaisquer dois modelos de Σ com cardinalidade κ são isomorfos, então Σ é completo.*

Prova. Sejam $\mathfrak{A}$ e $\mathfrak{B}$ modelos de Σ. Pelo Corolário 4.6.5, existem $\mathcal{L}$-estruturas $\mathfrak{A}_1$ e $\mathfrak{B}_1$ de cardinalidade κ com

$$\mathfrak{A} \equiv \mathfrak{A}_1 \quad \text{e} \quad \mathfrak{B} \equiv \mathfrak{B}_1,$$

em particular, $\mathfrak{A}_1$ e $\mathfrak{B}_1$ são modelos de Σ.

Daí, pela hipótese,

$$\mathfrak{A}_1 \cong \mathfrak{B}_1.$$

Em particular,

$$\mathfrak{A} \equiv \mathfrak{A}_1 \cong \mathfrak{B}_1 \equiv \mathfrak{B}.$$

e com isto $\mathfrak{A} \equiv \mathfrak{B}$. Com o Lema 4.12.12 obtemos a completude de Σ.

■

4.12.3 Modelo Completude

Nesta seção introduzimos uma propriedade das teorias, chamada modelo completude, com a ajuda da qual podemos provar a completude de algumas teorias. Para tal voltamos a utilizar o conjunto diagrama de uma estrutura (veja Definição 4.9.5).

Definição 4.12.14 *Um conjunto $\Sigma \subset Sent_{\mathcal{L}}$ chama-se modelo-completo se, para cada modelo $\mathfrak{A}$ de Σ, o conjunto das $\mathcal{L}(\mathfrak{A})$-sentenças $\Sigma \cup D(\mathfrak{A})$ é completo.*

Lema 4.12.15 *$\Sigma \subset Sent_{\mathcal{L}}$ é modelo completo se e somente se para quaisquer dois modelos $\mathfrak{A}, \mathfrak{B}$ de Σ que satisfazem $\mathfrak{A} \subset \mathfrak{B}$ também vale $\mathfrak{A} \prec \mathfrak{B}$.*

Prova. Seja Σ modelo completo. Sejam $\mathfrak{A}$ e $\mathfrak{B}$ modelos de Σ com $\mathfrak{A} \subset \mathfrak{B}$. Então fazem sentido as $\mathcal{L}(\mathfrak{A})$-estruturas

$$(\mathfrak{A}, |\mathfrak{A}|) \quad \text{e} \quad (\mathfrak{B}, |\mathfrak{A}|),$$

e elas são ambas modelos de $\Sigma \cup D(\mathfrak{A})$ pela Definição 4.8.1.

Assim, como Σ é modelo completo, pelo Lema 4.12.12 vale

$$(\mathfrak{A}, |\mathfrak{A}|) \equiv (\mathfrak{B}, |\mathfrak{A}|).$$

Pelo Corolário 4.9.8, isto tem como consequência

$$\mathfrak{A} \prec \mathfrak{B}.$$

Reciprocamente, suponhamos que vale $\mathfrak{A} \prec \mathfrak{B}$, sempre que $\mathfrak{A}$ e $\mathfrak{B}$ são modelos de Σ com $\mathfrak{A} \subset \mathfrak{B}$, fixamos um modelo $\mathfrak{A}$ de Σ e mostramos a completude de $\Sigma \cup D(\mathfrak{A})$.

Evidentemente $(\mathfrak{A}, |\mathfrak{A}|)$ é um modelo $\Sigma \cup D(\mathfrak{A})$. Queremos mostrar que cada outro modelo de $\Sigma \cup D(\mathfrak{A})$ é elementarmente equivalente a $(\mathfrak{A}, |\mathfrak{A}|)$.

Pelo Lema do Diagrama 4.9.6, um tal modelo contém uma imagem isomorfa a $\mathfrak{A}$. Identificamos $\mathfrak{A}$ com a sua imagem, e então podemos supor que o modelo considerado é da forma $(\mathfrak{B}, |\mathfrak{A}|)$, onde justamente vale $\mathfrak{A} \subset \mathfrak{B}$.

Como $\mathfrak{B}$ e $\mathfrak{A}$ são modelos de Σ, temos pela hipótese

$$\mathfrak{A} \prec \mathfrak{B}.$$

Pelo Corolário 4.9.8 vale portanto

$$(\mathfrak{A}, |\mathfrak{A}|) \equiv (\mathfrak{B}, |\mathfrak{A}|).$$

O Lema 4.12.12 nos garante então que $\Sigma \cup D(\mathfrak{A})$ é completo.

■

Uma teoria modelo-completa pode não ser completa, como pode ser encontrado em [11].

No entanto, se um sistema de axiomas modelo completo $\Sigma \subset Sent_{\mathcal{L}}$ possui um *modelo primo* então obtemos a completude de Σ.

Definição 4.12.16 *Chamamos uma $\mathcal{L}$-estrutura $\mathfrak{P}$ de modelo primo de um sistema de axiomas Σ caso $\mathfrak{P}$ é um modelo de Σ e existe uma imersão de $\mathfrak{P}$ em qualquer outro modelo de Σ.*

Corolário 4.12.17 *Se o conjunto $\Sigma \subset Sent_{\mathcal{L}}$ é modelo-completo e possui um modelo primo $\mathfrak{P}$ então Σ é completo.*

Prova. Sejam $\mathfrak{A}_1$ e $\mathfrak{A}_2$ modelos de Σ. Identificamos $\mathfrak{P}$ com a sua imersão em $\mathfrak{A}_1$ e $\mathfrak{A}_2$:

$$\mathfrak{P} \subset \mathfrak{A}_1 \quad \text{e} \quad \mathfrak{P} \subset \mathfrak{A}_2.$$

Como Σ é por hipótese modelo-completo segue pelo Lema 4.12.15 que $\mathfrak{P} \prec \mathfrak{A}_i$ para $i \in \{1, 2\}$. Em particular,

$$\mathfrak{A}_1 \equiv \mathfrak{P} \equiv \mathfrak{A}_2.$$

Logo Σ é completo pelo Lema 4.12.12.

■

Deduzimos agora um critério muito útil para garantir a modelo-completude de uma teoria. Começamos generalizando a Definição 4.10.11.

Definição 4.12.18 *Uma $\mathcal{L}$-fórmula chama-se existencial ou $\exists$-fórmula, caso seja da forma*

$$\exists x_1, ..., x_n \ \psi,$$

com ψ livre de quantificadores.

Analogamente, uma fórmula da forma

$$\forall x_1, ..., x_n \ \psi,$$

com ψ livre de quantificadores será chamada universal ou $\forall$-fórmula.

Observação 4.12.19 *A Definição 4.10.14 estabelece que uma $\mathcal{L}$-subestrutura $\mathfrak{A}$ de $\mathfrak{B}$ é dita existencialmente fechada em $\mathfrak{B}$ se cada sentença existencial da $\mathcal{L}(\mathfrak{A})$-linguagem que vale em $(\mathfrak{B}, |\mathfrak{A}|)$ também vale em $(\mathfrak{A}, |\mathfrak{A}|)$. Pelo Lema 4.9.3 isto é equivalente a dizer que para toda $\exists$−fórmula φ na $\mathcal{L}$−linguagem, e toda avaliação h em $\mathfrak{A}$,vale:*

$$\mathfrak{B} \models \varphi[h] \text{ implica } \mathfrak{A} \models \varphi[h].$$

Podemos agora enunciar o teorema.

Teorema 4.12.20 (Teste de Robinson) *Para $\Sigma \subset Sent_{\mathcal{L}}$ são equivalentes:*

(1) *Σ é modelo completo;*

(2) *para cada dois modelos $\mathfrak{A}, \mathfrak{B}$ de Σ com $\mathfrak{A} \subset \mathfrak{B}$, $\mathfrak{A}$ é existencialmente fechada em $\mathfrak{B}$;*

(3) *para cada $\mathcal{L}$-fórmula φ existe uma $\mathcal{L}$-fórmula universal ρ com $Fr(\rho) \subset Fr(\varphi)$, tal que*

$$\Sigma \vdash \forall(\varphi \leftrightarrow \rho).$$

Prova. (1) $\Rightarrow$ (2) segue imediato com o Lema 4.12.15.

(2) $\Rightarrow$ (3) : Consideramos inicialmente o caso em que φ é uma $\mathcal{L}$-fórmula existencial com $Fr(\varphi) \subset \{v_0, ..., v_n\}$. Aumentamos a linguagem $\mathcal{L}$ por novas constantes $c_0, ..., c_n$ (supondo, sem perda de generalidade, $\{0, ..., n\} \cap K = \emptyset$). Chamamos a linguagem aumentada de $\mathcal{L}'$. Seja φ' a $\mathcal{L}'$-sentença dada por

$$\varphi' = \varphi(v_0/c_0, ..., v_n/c_n).$$

Sejam $\mathfrak{A}', \mathfrak{B}'$ dois $\mathcal{L}'$-modelos de Σ com $\mathfrak{A}' \subset \mathfrak{B}'$. Para as $\mathcal{L}$-restrições $\mathfrak{A}$ e $\mathfrak{B}$ de $\mathfrak{A}'$ e $\mathfrak{B}'$ temos $\mathfrak{A} \subset \mathfrak{B}$ e portanto por hipótese $\mathfrak{A}$ é existencialmente fechada em $\mathfrak{B}$. Com o Lema 4.9.3 obtemos:

$$\mathfrak{B}' \models \varphi' \text{ implica } \mathfrak{A}' \models \varphi'.$$

Assim, pelo Teorema 4.12.11 existe uma $\mathcal{L}'$-fórmula δ' livre de quantificadores com

$$\Sigma \vdash (\varphi' \leftrightarrow \forall \delta').$$

Como $\forall \delta'$ é sentença podemos supor $Fr(\delta') \cap Fr(\varphi) = \emptyset$ (através de uma renomeação das variáveis de δ' se necessário). Definimos agora a $\mathcal{L}$-fórmula

$$\delta = \delta'(c_0/v_0, ..., c_n/v_n).$$

Aplicando o Lema 4.3.4 iteradamente e observando que as sentenças de Σ não envolvem as constantes $c_0, ..., c_n$ concluímos que

$$\Sigma \vdash (\varphi \leftrightarrow \forall\, x_1, ..., x_m\ \delta),$$

com $Fr(\delta') = \{x_1, ..., x_n\}$. Pelo Lema 4.2.9 (a), aplicado várias vezes, finalmente

$$\Sigma \vdash \forall(\varphi \leftrightarrow \forall\, x_1, ..., x_m\ \delta).$$

Com isto mostramos que, módulo "Σ", cada $\mathcal{L}$-fórmula existencial é equivalente a uma $\mathcal{L}$-fórmula universal.

Para mostrar a afirmação, falta ainda $Fr(\rho) \subset Fr(\varphi)$ para ρ como em (3). Mostramos isto através de indução sobre a construção de qualquer

$\mathcal{L}$-fórmula φ. Note que pelo Lema 4.2.9 (a)

$$\Sigma \vdash \forall(\varphi \leftrightarrow \rho) \quad \text{se e só se} \quad \Sigma \vdash (\varphi \leftrightarrow \rho).$$

Portanto, no que segue basta provar o resultado para a parte direita da equivalência acima.

- Se φ é uma fórmula atômica, definimos $\rho = \varphi$.

- Se $\varphi = \neg\varphi_1$ e por hipótese de indução

$$\Sigma \vdash (\varphi_1 \leftrightarrow \rho_1) \quad \text{com} \quad Fr(\rho_1) \subset Fr(\varphi_1)$$

com ρ_1 universal, então vale naturalmente também

$$\Sigma \vdash (\neg\varphi_1 \leftrightarrow \neg\rho_1).$$

Claramente $\neg\rho_1$ é uma $\mathcal{L}$-fórmula existencial (ao menos equivalente a uma). Pelo que vimos no início desta prova, existe uma $\mathcal{L}$-fórmula universal ρ equivalente a $\neg\rho_1$ com $Fr(\rho) \subset Fr(\neg\rho_1)$.

Assim obtemos

$$\Sigma \vdash (\neg\varphi_1 \leftrightarrow \rho)$$

com $Fr(\rho) \subset Fr(\neg\varphi_1)$.

- Se $\varphi = (\varphi_1 \wedge \varphi_2)$ e por hipótese de indução, para $i = 1, 2$;

$$\Sigma \vdash (\varphi_i \leftrightarrow \rho_i) \quad \text{com} \quad Fr(\rho_i) \subset Fr(\varphi_i)$$

e ρ_i universal, então vale

$$\Sigma \vdash ((\varphi_1 \wedge \varphi_2) \leftrightarrow (\rho_1 \wedge \rho_2)).$$

Por um raciocínio puramente lógico $(\rho_1 \wedge \rho_2)$ é novamente equivalente a uma ρ universal com $Fr(\rho_1 \wedge \rho_2) \subset Fr(\rho)$. Assim obtemos finalmente

$$\Sigma \vdash (\varphi \leftrightarrow \rho) \quad \text{com} \quad Fr(\varphi) \subset Fr(\rho).$$

- Se $\varphi = \forall x\ \varphi_1$ e por hipótese de indução

$$\Sigma \vdash (\varphi_1 \leftrightarrow \rho_1) \quad \text{com} \quad Fr(\rho_1) \subset Fr(\varphi_1)$$

e ρ_1 universal, então segue imediatamente

$$\Sigma \vdash (\forall x\ \varphi_1 \leftrightarrow \forall x\ \rho_1).$$

Tomando $\rho = \forall x\ \rho_1$ temos $Fr(\forall x\ \rho_1) = Fr(\rho) \subset Fr(\forall x\ \varphi_1)$. E claramente (3) fica provado.

(3) $\Rightarrow$ (1) : Utilizamos aqui o Lema 4.12.15 para provar a afirmação. Sejam $\mathfrak{A}$ e $\mathfrak{B}$ modelos de Σ com $\mathfrak{A} \subset \mathfrak{B}$. Queremos mostrar então que $\mathfrak{A} \prec \mathfrak{B}$. Agora seja φ uma $\mathcal{L}$-fórmula e h uma avaliação em $\mathfrak{A}$. Por (3) existe uma $\mathcal{L}$-fórmula ρ universal com

$$\Sigma \vdash (\varphi \leftrightarrow \rho).$$

De

$$\mathfrak{B} \models \varphi[h]$$

segue portanto

$$\mathfrak{B} \models \rho[h].$$

Isto tem como consequência imediata

$$\mathfrak{A} \models \rho[h],$$

por causa da universalidade de ρ. Mas isto também é equivalente a

$$\mathfrak{A} \models \varphi[h].$$

Com isto mostramos, pela Definição 4.8.4, $\mathfrak{A} \prec \mathfrak{B}$.

■

5 A Conjectura de Artin e o Teorema de Ax. e Kochen

5.1 Prova do Teorema de Ax. e Kochen

Dado um corpo K, dizemos que K é um C_2-corpo se todo polinômio homogêneo de grau total d em mais de d^2 variáveis e com coeficientes em K admite uma solução não trivial em K. Em 1936, Chevalley mostrou que, em todo corpo finito, todo polinômio homogêneo com mais variáveis que seu grau total possui raiz nele mesmo (veja [2]).

Definição 5.1.1 *Dizemos que K é um corpo $C_i(d)$ se todo polinômio homogêneo de grau total d em mais de d^i variáveis e com coeficientes em K admite uma solução não trivial em K. O corpo K é dito ainda um C_i-corpo se for $C_i(d)$ para todo $d \in \mathbb{N}^*$.*

Assim, todo corpo finito é C_1. O Lema de Hensel (veja Teorema 3.2.13) nos permite provar que toda forma quadrática em mais do que $4 = 2^2$ variáveis e com coeficientes em qualquer corpo $p-$ádico $\mathbb{Q}_p$ admite solução não trivial em $\mathbb{Q}_p$. D.J. Lewis mostrou em 1952 (veja [9]) um resultado análogo para as formas cúbicas, isto é, que toda forma cúbica em mais do que $9 = 3^2$ variáveis e com coeficientes em qualquer corpo $p-$ádico $\mathbb{Q}_p$ admite solução não trivial em $\mathbb{Q}_p$. Assim, $\mathbb{Q}_p$ é $C_2(2)$ e $C_2(3)$.

Em 1963, Lang mostrou que se K é um corpo C_i então o corpo $K((X))$ das séries formais de Laurent sobre K

$$K((X)) = \left\{ \sum_{i=m}^{\infty} a_i X^i;\ m \in \mathbb{Z} \ \text{ e } \ a_i \in k \ \text{ para todo } i \geq m \right\}$$

é C_{i+1} (veja [8]), e portanto, em particular, os corpos $\mathbb{F}_p((X))$ são C_2.

Baseado na semelhança entre os corpos $\mathbb{Q}_p$ dos números $p-$ádicos e $\mathbb{F}_p((X))$ (ambos são corpos valorizados henselianos com grupo de valores $\mathbb{Z}$ e corpo de resíduos $\mathbb{F}_p$); a diferença essencial entre ambos se resume à característica: enquanto a característica de $\mathbb{F}_p((X))$ é prima, a carac-

terística de $\mathbb{Q}_p$ é zero), Artin conjecturou então que o corpo $\mathbb{Q}_p$ deveria ser também C_2.

Esta conjectura revelou-se "quase" verdadeira: em 1965, Ax e Kochen mostraram (veja [1]) que para todo grau d fixado, tem-se que é finito o conjunto dos primos p tais que $\mathbb{Q}_p$ não é $C_2(d)$. Mais precisamente:

Teorema (Ax-Kochen, 1965): Para cada grau $d \in \mathbb{N}^*$ existe uma cota n_d tal que, para todo primo $p \geq n_d$, $\mathbb{Q}_p$ é um corpo $C_2(d)$, ou seja, cada polinômio homogêneo de grau d em mais de d^2 indeterminadas reproduz o zero de forma não-trivial.

Nosso objetivo agora é abordar a Teoria de Modelos dos corpos henselianos e finalmente discutir a Conjectura de Artin e sua resolução.

Inicialmente salientamos que a classe dos corpos henselianos na linguagem de corpos, com a adicional relação unária V, é axiomatizável: para isto apresentamos o seguinte sistema de axiomas para os corpos henselianos na linguagem de corpos (veja Exemplo 4.5.11(4)):

$$\Sigma = \{K_0 - K_9, V_1 - V_3\} \cup \{H_n \mid n \in \mathbb{N}\}.$$

No que segue exploramos o fato importante de que na linguagem de um corpo valorizado $(F, \mathcal{O})$ também podemos falar sobre o seu corpo de resíduos $\overline{F}$ e seu grupo de valores Γ. Para isto, precisamos fazer uma tradução das fórmulas escritas na linguagem de corpos e na linguagem de grupos. No que segue, mantemos em mente as seguintes representações do corpo de resíduos e do grupo de valores:

$$\overline{F} = \mathcal{O}/\mathcal{M} \quad , \quad \Gamma = K^\times/\mathcal{O}^\times.$$

Começamos com o corpo de resíduos: efetuamos a "tradução" φ_r de uma fórmula φ da linguagem de corpos. Fazemos isto por indução sobre a

construção da fórmula da seguinte maneira:

$$(t_1 \doteq t_2)_r := \neg V^\times(t_1 - t_2), \tag{98}$$

$$(\neg\varphi)_r := \neg\varphi_r, \tag{99}$$

$$(\varphi \wedge \psi)_r := (\varphi_r \wedge \psi_r), \tag{100}$$

$$(\forall x\ \varphi)_r := \forall x\ (V(x) \rightarrow \varphi_r). \tag{101}$$

Lembramos que, como no Exemplo 4.5.11, definimos $V^\times(z)$ como sendo a fórmula

$$V(z) \wedge \exists y\ (yz \doteq 1 \wedge V(y)),$$

a qual nos diz que $z \in \mathcal{O}^\times$.

A definição em (98) nos diz, por exemplo, que dois elementos do corpo de resíduos são iguais se, e somente se, a sua diferença não é uma unidade no anel de valorização, o que condiz com o que já sabemos de corpos valorizados. As traduções em (99) e (100) são as mais óbvias possíveis. Em (101) é necessário introduzir a fórmula $(V(x) \rightarrow \varphi_r)$ pois os elementos do corpo de resíduos provêm do anel de valorização, e o quantificador " $\forall\ x$ " , como já sabemos, quantifica sobre o corpo inteiro que contém este anel. Claramente conseguimos traduzir todas as fórmulas a partir das acimas listadas.

Para toda fórmula φ com $Fr(\varphi) = \{v_0, .., v_n\}$ temos que $Fr(\varphi_r) = \{v_0, .., v_n\}$. De fato, isto segue observando que em (98)-(101) os dois lados das equações têm as mesmas variáveis livres. Mais ainda, para todo corpo valorizado $(F, \mathcal{O})$, se $a_1, ..., a_n \in \mathcal{O}$, então vale, usando a Notação 4.7.6:

$$\overline{F} \models \varphi[\overline{a_0}, ..., \overline{a_n}] \quad \text{se só se} \quad (F, \mathcal{O}) \models \varphi_r[a_0, ..., a_n]; \tag{102}$$

o que se mostra por indução sobre a construção das fórmulas.

A "tradução" φ_g de uma fórmula φ da linguagem de grupos ordenados, com a operação do grupo $\Gamma = K^\times/\mathcal{O}^\times$ escrita excepcionalmente de maneira

multiplicativa, é efetuada da seguinte forma:

$$(t_1 \doteq t_2)_g := \exists x\ (V^\times(x) \wedge x \cdot t_1 \doteq t_2), \tag{103}$$

$$(t_1 < t_2)_g := \exists x\ (V(x) \wedge \neg V^\times(x) \wedge x \cdot t_1 \doteq t_2), \tag{104}$$

$$(\neg\varphi)_g := \neg\varphi_g, \tag{105}$$

$$(\varphi \wedge \psi)_g := (\varphi_g \wedge \psi_g), \tag{106}$$

$$(\forall x\ \varphi)_g := \forall x\ (x \neq 0 \rightarrow \varphi_g), \tag{107}$$

onde, nos casos (103) e (104), a variável x não ocorre em t_1 nem em t_2.

O que está escrito em (103) é, precisamente, que elementos iguais no grupo de valores diferem pela multiplicação de uma unidade do anel de valorização. Em (104), o que se lê é que um elemento é menor que outro se, e somente se, existe um elemento do ideal maximal que multiplicando o menor é igual ao maior. Temos traduções canônicas em (105) e (106). E, finalmente, em (107) nos livramos do problema com a quantificação, lembrando que os elementos do grupo de valores são originados de $K^\times$.

Analogamente ao que vimos para corpos, se φ é uma fórmula com $Fr(\varphi) = \{v_0, ..., v_n\}$ então $Fr(\varphi_g) = \{v_0, ..., v_n\}$ e, para todo corpo valorizado $(F, \mathcal{O})$, se $a_0, ..., a_n \in F^\times$ então

$$\Gamma \models \varphi[a_0\mathcal{O}^\times, ..., a_n\mathcal{O}^\times] \quad \text{se e só se} \quad (F, \mathcal{O}) \models \varphi_g[a_0, ..., a_n], \tag{108}$$

novamente usando a Notação 4.7.6. Isto se prova por indução sobre a construção das fórmulas.

Lema 5.1.2 *Se $(F, \mathcal{O})$ é κ-saturado então o seu corpo de resíduos $\overline{F}$ e o seu grupo de valores Γ são κ-saturados.*

Prova. *$\overline{F}$ é κ-saturado*: Seja $\Phi(v_0)$ um Tipo de $\overline{F}$. Pelo Lema 4.10.5 todo subconjunto finito de $\Phi(v_0)$ é realizável, digamos, por $\overline{\alpha} \in \overline{F}$. Portanto, por (102) todo subconjunto finito do correspondente conjunto $\Phi_r(v_0) := \{\varphi_r \mid \varphi \in \Phi\}$ é também realizável, a saber, pelo correspondente representante α. Salientamos que por (102) também vale a recíproca, ou seja, se

$\Phi_r(v_0)$ é realizável então $\Phi(v_0)$ também o é. Assim $\Phi_r(v_0)$ é um Tipo de $(F, \mathcal{O})$ pelo Lema 4.10.5.

Se $\mathsf{card}(\Phi(v_0)) < \kappa$ então $\mathsf{card}(\Phi_r(v_0)) < \kappa$. Como $(F, \mathcal{O})$ é κ-saturado, concluímos que $\Phi_r(v_0)$ é realizável em F. E pelo visto acima, $\Phi(v_0)$ é realizável por um $\overline{a} \in \overline{F}$. Logo $\overline{F}$ é κ-saturado.

Γ é *κ-saturado*: Segue análogo a prova da saturação de $\overline{F}$, agora observando a equivalência em (108).

■

Teorema 5.1.3 *Seja $(F, \mathcal{O})$ um corpo valorizado henseliano com grupo de valores Γ e corpo de resíduos $\overline{F}$. Seja $(F_1, \mathcal{O}_1)$ uma extensão de $(F, \mathcal{O})$, como corpo valorizado, com grupo de valores Γ_1 e corpo de restos $\overline{F_1}$. Se:*

(a) $car(\overline{F}) = 0$.

(b) Γ *é existencialmente fechado em* Γ_1. *(como grupo ordenado.)*

(c) $\overline{F}$ *é existencialmente fechado em* $\overline{F_1}$. *(como corpo.)*

então $(F, \mathcal{O})$ é existencialmente fechado em $(F_1, \mathcal{O}_1)$.

Prova. Seja $(F_2, \mathcal{O}_2)$ uma extensão elementar κ^+-saturada de $(F, \mathcal{O})$ com $\kappa = \mathsf{card}(F_1)$. Uma tal extensão existe pelo Teorema da Existência 4.10.9.

Mostraremos que $(F_1, \mathcal{O}_1)$ pode ser imersa em $(F_2, \mathcal{O}_2)$ sobre $(F, \mathcal{O})$ (isto é, que tal imersão é a identidade quando restrito a F), pois pelo Corolário 4.10.15 (2) a estrutura $(F, \mathcal{O})$ é existencialmente fechada em $(F_1, \mathcal{O}_1)$.

Pelo Lema 5.1.2, o corpo de restos $\overline{F_2}$ e o grupo de valores Γ_2 de $(F_2, \mathcal{O}_2)$ são também κ^+-saturados. Com o Corolário 4.10.15 (1) segue portanto da hipótese do teorema que o corpo de restos $\overline{F_1}$ e o grupo de valores Γ_1 de $(F_1, \mathcal{O}_1)$ podem ser imersos no corpo de restos $\overline{F_2}$ e no grupo de valores Γ_2 de $(F_2, \mathcal{O}_2)$, respectivamente. Identificando as imagens, podemos supor daqui por diante $\overline{F_1} \subset \overline{F_2}$ e $\Gamma_1 \subset \Gamma_2$.

Podemos supor que $(F_1, \mathcal{O}_1)$ e $(F_2, \mathcal{O}_2)$ são henselianos. De fato, $(F_2, \mathcal{O}_2)$ já é henseliano pois é uma extensão elementar do corpo henseliano $(F, \mathcal{O})$.

E e $(F_1, \mathcal{O}_1)$ não é henseliano, podemos tomar a sua henselização, a qual não muda as hipóteses sobre o corpo de restos e o grupo de valores, pois pelo Teorema 3.6.7 a henselização é uma extensão imediata.

Encontramo-nos então diante da seguinte situação:

$$\begin{array}{ccc} (F_1, \mathcal{O}_1) & & (F_2, \mathcal{O}_2) \\ | & & | \\ (F, \mathcal{O}) & \xrightarrow{id} & (F, \mathcal{O}) \end{array}$$

onde $(F_1, \mathcal{O}_1)$ e $(F_2, \mathcal{O}_2)$ são henselianos e $(F_2, \mathcal{O}_2)$ é $\mathsf{card}(F_1)^+$-saturada e as seguintes condições valem, além de $(a), (b)$ e (c):

(i) $(F, \mathcal{O})$ é henseliano,

(ii) $\overline{F} \subset \overline{F_1} \subset \overline{F_2}$,

(iii) $\Gamma \subset \Gamma_1 \subset \Gamma_2$ e Γ é puro em Γ_1, ou seja , se $n\gamma_1 \in \Gamma$ para um $\gamma_1 \in \Gamma_1$ e um $n \geq 1$, então $\gamma_1 \in \Gamma$,

sendo que a condição em (iii) segue de (c) levando em conta a seguinte sentença existencial da linguagem de Γ_1

$$\exists x \underbrace{x + ... + x}_{\text{n-vezes}} \doteq \underline{\gamma}$$

- *Afirmação*: Se $(F_2, \mathcal{O}_2)$ é $\mathsf{card}(F_1)^+$-saturada e $(i), (ii)$ e (iii) são satisfeitas então $(F_1, \mathcal{O}_1)$ pode ser imersa em $(F_2, \mathcal{O}_2)$ sobre $(F, \mathcal{O})$.

Com a ajuda do Lema de Zorn (e identificando imagens) podemos supor que a imersão id de $(F, \mathcal{O})$ é maximal com as propriedades $(i) - (iii)$.

Basta então mostrar que $F = F_1$.

Supomos $F \neq F_1$ e distinguimos três casos.

- *Caso 1* : $\overline{F} \subsetneq \overline{F_1}$.

Tomamos algum $x_1 \in F_1$ com $\overline{x_1} \in \overline{F_1} \backslash \overline{F}$. Por (ii), existe $x_2 \in F_2$ tal que $\overline{x_2} = \overline{x_1}$.

Daqui em diante utilizaremos a "barra" para a aplicação de tomar classe de restos tanto para $\mathcal{O}_1$ como também para $\mathcal{O}_2$, enquanto isto não levar a confusões.

- *Caso 1.a* : $\overline{x_1}$ é transcendente sobre $\overline{F}$.

$$\begin{array}{ccc} (F_1, \mathcal{O}_1) & & (F_2, \mathcal{O}_2) \\ | & & | \\ (F_1' = F(x_1), \mathcal{O}') & \hookleftarrow & | \\ | & & | \\ (F, \mathcal{O}) & \xrightarrow{\quad id \quad} & (F, \mathcal{O}) \end{array}$$

De fato, inicialmente salientamos que se $x_2 \in F_2$ com $\overline{x_2} = \overline{x_1}$, pelo Teorema 3.5.18 (2), x_1 e x_2 são transcendentes sobre F.

Como $\overline{x_1} \neq \overline{0}$ e $\overline{x_2} \neq \overline{0}$ nos seus respectivos anéis de valorização, temos $v_1(x_1) = 0$ e $v_2(x_2) = 0$. Assim, pelo Corolário 3.5.14, as valorizações induzidas por $\mathcal{O}_1$ e $\mathcal{O}_2$ são dadas por: para $a_0, ..., a_n \in F$ e $\nu \in \{1, 2\}$,

$$v_\nu(a_0 + ... + a_n x_\nu^n) = \min\{v(a_i) \mid 0 \leq i \leq n\}.$$

Ainda pelo Corolário 3.5.14, vale para os grupos de valores Γ_ν' e para os corpos de restos $\overline{F}_\nu'$ das restrições $\mathcal{O}_\nu'$ de $\mathcal{O}_\nu$ sobre $F_\nu' = F(x_\nu)$, onde $\nu \in \{1, 2\}$:

$$\Gamma_1' = \Gamma = \Gamma_2' \quad \text{e} \quad \overline{F(x_1)} = \overline{F}(\overline{x_1}) = \overline{F}(\overline{x_2}) = \overline{F(x_2)}.$$

Portanto, a aplicação σ definida por $a \mapsto a$ para $a \in F$ e $x_1 \mapsto x_2$, define um isomorfismo sobre $(F, \mathcal{O})$ entre $(F_1', \mathcal{O}_1 \cap F_1')$ e $(F_2', \mathcal{O}_2 \cap F_2')$ que conjuga os anéis de valorização.

Portanto, os corpos valorizados $(F_1', \mathcal{O}_1 \cap F_1')$ e $(F_2', \mathcal{O}_2 \cap F_2')$ são extensões próprias de $(F, \mathcal{O})$ satisfazendo (ii) e (iii). Tomando os fechos henselianos de ambos, obtemos (i) e não perdemos a validade de (ii) e (iii) graças à propriedade que tem a henselização de ser extensão imediata. Porém, isto contradiz a maximalidade da imersão em F_2 acima suposta. Assim $\overline{F_1}|\overline{F}$ é

algébrica.

Observamos agora que

$$\overline{F} \text{ existencialmente fechado em } \overline{F}_1 \Rightarrow \overline{F} \text{ algebricamente fechado em } \overline{F}_1,$$

e portanto, uma vez que estamos supondo $\overline{F} \subsetneq \overline{F}_1$, então necessariamente $\overline{F}_1|\overline{F}$ é transcendente. Assim, como $\overline{x}_1 \in \overline{F}_1 \backslash \overline{F}$, temos $\overline{x}_1$ é transcendente sobre $\overline{F}$, o que nos leva a um absurdo, e portanto teríamos encerrado a prova do *Caso 1* aqui. No entanto, vamos esquecer esta hipótese a fim de poder enunciar após o Lema 5.1.4, cuja prova está contida nesta. Assim, temos mais um caso a considerar.

Caso 1.b: $\overline{x_1} \notin \overline{F}$, mas é algébrico sobre $\overline{F}$.

Queremos aqui também chegar a uma contradição construindo uma extensão própria de $(F, \mathcal{O})$ em $(F_1, \mathcal{O}_1)$ satisfazendo $(i), (ii)$ e (iii) e uma imersão desta em $(F_2, \mathcal{O}_2)$.

Seja $f_1(X) \in \mathcal{O}[X]$ mônico, tal que

$$\overline{f_1} = Irr(\overline{x_1}, \overline{F}).$$

Então $f_1(X)$ é irredutível sobre $F[X]$ (veja as considerações depois da prova do Lema 3.6.2). Como $\mathsf{car}(\overline{F}) = 0$, temos que $\overline{x_1}$ é um zero simples de $\overline{f_1}$ em $\overline{F}$, já que em todo corpo de característica zero todo polinômio irredutível é separável.

Como $\overline{f_1} \in \overline{F}[X] \subset \overline{F_1}[X] \subset \overline{F_2}[X]$, pelo Lema de Hensel (Teorema 3.6.4(4)), já que F_1 e F_2 são henselianos,

$$\exists \alpha_1 \in \mathcal{O}_1,\ f_1(\alpha_1) = 0 \text{ e } \overline{\alpha_1} = \overline{x_1},$$
$$\exists \alpha_2 \in \mathcal{O}_2,\ f_1(\alpha_2) = 0 \text{ e } \overline{\alpha_2} = \overline{x_1}.$$

Portanto, existe um isomorfismo $\widetilde{\sigma}$ sobre F entre os corpos $F(\alpha_1)$ e $F(\alpha_2)$.

$$\begin{array}{ccc} F_1 & & F_2 \\ | & & | \\ F(\alpha_1) & \xrightarrow{\widetilde{\sigma}} & F(\alpha_2) \\ | & & | \\ F & \xrightarrow{id=\sigma} & F \end{array}$$

O isomorfismo $\widetilde{\sigma}$ preserva a valorização. De fato, F é henseliano, e portanto $\mathcal{O}$ se estende unicamente para os anéis de valorização $\mathcal{O}_{F(\alpha_1)}$ e $\mathcal{O}_{F(\alpha_2)}$ de $F(\alpha_1)$ e $F(\alpha_2)$, respectivamente. Como $\widetilde{\sigma}(\mathcal{O}_{F(\alpha_1)})$ é um anel de valorização de $F(\alpha_2)$ que estende $\mathcal{O}$, temos que $\widetilde{\sigma}(\mathcal{O}_{F(\alpha_1)}) = \mathcal{O}_{F(\alpha_2)}$.

Verificamos agora que temos (i), (ii) e (iii), assim chegando a uma contradição com o caráter maximal de F.

(i): $F(\alpha_1)$ e $F(\alpha_2)$ são extensões algébricas do corpo henseliano F, e portanto também são henselianos.

(ii): Como $F(\alpha_1)|F$ e $F(\alpha_2)|F$ são algébricas, tomando Γ_{α_1} e Γ_{α_2} como os correspondentes grupos de valores, a Proposição 3.5.11 implica que, para $i \in \{1, 2\}$,

$$[\overline{F(\alpha_i)} : \overline{F}].[\Gamma_{\alpha_i} : \Gamma] \leq [F(\alpha_1) : F] = \deg(f_1). \tag{109}$$

Observamos agora que $\overline{f_1}$ tem o mesmo grau que f_1, pois f_1 é mônico, e são ambos irretdutíveis, então

$$[\overline{F}\ (\overline{x_1}) : \overline{F}] = \deg(f_1).$$

Assim, já que

$$\overline{F}\ (\overline{x_1}) = \overline{F}\ (\overline{\alpha_i}) \subseteq \overline{F(\alpha_i)},$$

e segue de (109) que

$$\overline{F(\alpha_1)} = \overline{F}\ (\overline{\alpha_1}) = \overline{F}(\overline{x}_1) = \overline{F}\ (\overline{\alpha_2}) = \overline{F(\alpha_2)}, \quad \text{e} \quad [\overline{F(\alpha_i)} : \overline{F}] = \deg(f_1). \tag{110}$$

(*iii*): De (109) e (110) segue que $[\Gamma_{a_i} : \Gamma] = 1$, e então $\Gamma_{a_i} = \Gamma$, o que conclui a prova do *Caso 1*.

Caso 2 : $\overline{F} = \overline{F_1}$ e $\Gamma \subsetneq \Gamma_1$.

Novamente vamos chegar a um absurdo ao conseguir estender a identidade.

Tomamos $\gamma \in \Gamma_1 \backslash \Gamma$ e $x_1 \in F_1$ com $v_1(x_1) = \gamma$. Temos que x_1 é transcendente sobre F, pois Γ é puro em Γ_1 (portanto não existe extensão própria Γ_{x_1} de Γ tal que $[\Gamma_{x_1} : \Gamma]$ é finita). Como vale (*iii*), pelo Corolário 3.5.16, o grupo de valores da restrição de $\mathcal{O}_1$ sobre $F(x_1)$ é $\Gamma \oplus \mathbb{Z}\gamma$, seu corpo de resíduos é $\overline{F}$ e, para $a_0, ..., a_n \in F$, vale

$$v_1(a_n x_1^n + ... + a_0) = \min\{v(a_i) + i \underbrace{v_1(x_1)}_{\gamma} \mid 0 \leq i \leq n\}.$$

Assim, a restrição $\mathcal{O}_1'$ de $\mathcal{O}_1$ sobre o corpo intermediário $F_1' = F(x)$ tem como grupo de valores $\Gamma \oplus \mathbb{Z}\gamma$ e seu corpo de resíduos permanece $\overline{F}$. Pelo Corolário 3.5.19, x_1 é transcendente sobre F.

$$\begin{array}{ccc} F_1 & & F_2 \\ | & & | \\ F_1' = F(x_1) & & | \\ | & & | \\ F & \xrightarrow{\sigma} & F \end{array}$$

Tomamos agora $x_2 \in F_2$ tal que $v_2(x_2) = \gamma$. Novamente x_2 é transcendente sobre F com corpo de resíduos $\overline{F}$, grupo de valores $\Gamma \oplus \mathbb{Z}\gamma$ e satisfazendo para $a_0, ..., a_n \in F$

$$v_2(a_n x_2^n + ... + a_0) = \min\{v(a_i) + i \underbrace{v_2(x_2)}_{\gamma} \mid 0 \leq i \leq n\}.$$

A aplicação σ' definida por $a \mapsto a$ para $a \in F$ e $x_1 \mapsto x_2$, define então uma imersão

$$\sigma' : F_1' = F(x_1) \to F(x_2) = F_2'$$

que preserva a valorização e é a identidade sobre F.

Procuramos agora por extensões algébricas F_1'' de F_1' e F_2'' de F_2' e uma extensão σ'' de σ' tal que Γ_1'' seja puro em Γ, pois com isto, garantimos (iii). Como (ii) é automaticamente satisfeita garantimos (i) tomando sua heselização.

Afirmamos que o fecho algébrico de $F(x_1)$ em F_1 satisfaz esta condição.

Seja F_1'' o fecho algébrico de $F(x_1)$ em F_1. Suponha por absurdo que Γ_1'' não é puro em Γ_1, ou seja, existe um número primo q e um $\delta \in \Gamma_1 \backslash \Gamma_1''$ tal que

$$q\delta \in \Gamma_1''.$$

Vamos construir uma extensão própria de F_1' de grau q contida em F_1 e chegar numa contradição.

Se existe $\delta \in \Gamma_1 \backslash \Gamma_1''$ tal que $q\delta \in \Gamma_1''$ então existem $y \in F_1 \backslash F_1''$ e $a \in F_1''$ com

$$v_1(y) = \delta \quad \text{e} \quad v_1(a) = q\delta = qv_1(y) = v_i(y^q).$$

Portanto vale

$$v_1(y^q a^{-1}) = 0.$$

Assim $y^q a^{-1}$ é uma unidade de $\mathcal{O}_1$ e como $\overline{F} = \overline{F}_1$, temos $\overline{F_1} = \overline{F_1''}$ de modo que existe um $c \in F_1''$ com $c \neq 0$ e

$$\overline{y^q a^{-1}} = \overline{c},$$

e então

$$\overline{y^q a^{-1} c^{-1}} = \overline{1}.$$

Como $\mathsf{car}(\overline{F_1}) = 0$ e q é primo, temos que o polinômio

$$X^q - y^q a^{-1} c^{-1} \in \mathcal{O}_1[X]$$

tem um zero simples em $\overline{F_1}$.

A propriedade henseliana de $(F_1, \mathcal{O}_1)$ (Teorema 3.6.4(4)) assegura com isto a existência de um $z \in \mathcal{O}_1^\times$ com

$$z^q = y^q a^{-1} c^{-1}.$$

Assim ac é uma q-ésima potência em F_1. Com isto é claro que $F_1''(yz^{-1})$ é uma extensão algébrica de F_1''. Como $yz^{-1} \in F_1$ e F_1'' é o fecho algébrico de F_1' em F_1, temos que $yz^{-1} \in F_1''$. Mas então

$$v_1(yz^{-1}) = v_1(y) - v_1(z) \overset{z \in \mathcal{O}_1^\times}{=} \delta - 0 \in \Gamma_1'',$$

uma contradição.

Assim, temos que

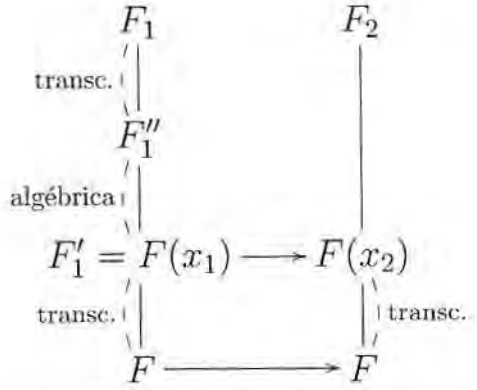
$$(F_1'', \mathcal{O}_1'')$$

é uma extensão algébrica de $(F_1', \mathcal{O}_1')$ com

$$\mathcal{O}_1'' = \mathcal{O}_1 \cap F_1'',$$

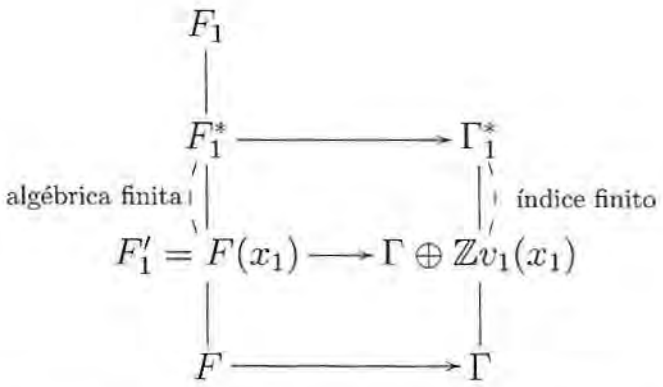
e cujo grupo de valores Γ'' é puro em Γ_1.

Afirmamos agora que é possível imergir o corpo valorizado $(F_1'', \mathcal{O}_1'')$ em $(F_2, \mathcal{O}_2)$ sobre $(F, \mathcal{O})$ preservando os anéis de valorização. Estamos assim na situação:



Pela $\mathsf{card}(F_1)^+$-saturabilidade de $(F_2, \mathcal{O}_2)$ basta, pelo Corolário 4.10.15 (1), mostrar que podemos imergir cada extensão finitamente gerada $F_1^* \subset F_1$ de F_1' em F_2 sobre F_1'.

Temos a seguinte situação:



Sem perda de generalidade podemos supor $\Gamma \subsetneq \Gamma^*$. Como

$$\frac{\Gamma_1^*}{\Gamma \oplus \mathbb{Z}\gamma} \simeq \frac{\Gamma_1^*/\Gamma}{(\Gamma \oplus \mathbb{Z}\gamma)/\Gamma} \simeq \frac{\Gamma_1^*/\Gamma}{\mathbb{Z}},$$

vale

$$[(\Gamma_1^*/\Gamma) : \mathbb{Z}] < \infty,$$

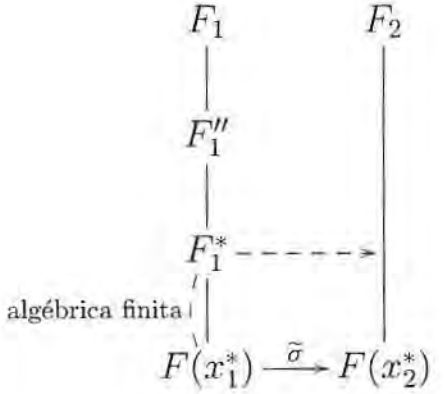
uma vez que a extensão é algébrica finita, e então $\Gamma_1^*/\Gamma \simeq \mathbb{Z}$. Como Γ é puro em Γ_1 e $\Gamma \subset \Gamma_1^* \subset \Gamma_1$, temos que Γ é puro em Γ_1^*; assim, existem $\gamma^* \in \Gamma_1^*$ e $x_1^* \in F_1^*$ com $v_1(x_1^*) = \gamma^*$, tais que

$$\Gamma_1^* = \Gamma \oplus \mathbb{Z}\gamma^* = \Gamma \oplus \mathbb{Z}v_1(x_1^*),$$

com x_1^* transcendente sobre F (caso contrário a soma não seria direta) e

$$[F_1^* : F(x_1^*)] < \infty.$$

Construímos uma imersão de $F(x_1^*)$ (ao invés de $F(x_1)$).



Escolha x_2^* tal que $v_2(x_2^*) = \gamma^* = v_1(x_1^*)$. Então $\widetilde{\sigma}|_F = id$ e $\widetilde{\sigma}(x_1^*) = x_2^*$ define uma imersão sobre F que preserva os anéis de valorização pois

$$v_1(a_n(x_1^*)^n + ... + a_0) = \min\{v(a_i) + i\gamma^* \mid 0 \leq i \leq n\} = v_2(a_n(x_2^*)^n + ... + a_0),$$

e também

$$\overline{F_1} \overset{Hip.}{=} \overline{F} = \overline{F(x_1^*)} = \overline{F(x_2^*)},$$

sendo assim $F_1^*|F(x_1^*)$ imediata e algébrica. Como $\mathsf{car}(\overline{F}) = 0$, $F(x_1^*)$ é finitamente ramificado, e assim, pelo Corolário 3.6.17, a henselização de $F(x_1^*)$ é algébrica maximal, e daí F_1^* deve estar contido nela. Novamente conseguimos estender $\widetilde{\sigma}$ para uma imersão da henselização de $F(x_1^*)$, a qual satisfaz (i), (ii) e (iii), o que leva a uma contradição com o caráter maximal de F.

Caso 3 : $\overline{F} = \overline{F_1}$ e $\Gamma = \Gamma_1$ (isto é, a extensão $(F_1, \mathcal{O}_1)|(F, \mathcal{O})$ é imediata.)

Seja $x_1 \in F_1 \backslash F$. Podemos supor que o elemento x_1 é transcendente sobre F, pois caso contrário, pelas hipóteses, bastaria tomar a henselização de $F(x_1)$ para encontrar via a κ-saturação de F_2 usando o polinômio irredutível de x_1 uma imersão da extensão própria $F(x_1)|F$ em F_2 com as propriedades (i), (ii) e (iii).

Vamos mostrar que existe $x_2 \in F_2 \backslash F$ com

$$v_1(x_1 - a) = v_2(x_2 - a) \tag{111}$$

para todo $a \in F$.

Para obtermos a existência de $x_2 \in F_2$ satisfazendo (111), empregamos a κ^+-saturação de $(F_2, \mathcal{O}_2)$. Mostramos então que o seguinte conjunto de fórmulas é um tipo de $(F_2, \mathcal{O}_2)$:

$$\Phi(z_0) = \{\neg((z_0 - \underline{a}) < \underline{b_a})_g \wedge \neg(\underline{b_a} < (z_0 - \underline{a}))_g \ ; \ a \in F\},$$

onde $b_a \in F$ é tal que $v(b_a) = v_1(x_1 - a)$, o qual existe pois $\Gamma = \Gamma_1$.

Pelo Lema 4.10.5 basta verificarmos que cada subconjunto finito de $\Phi(z_0)$ é realizável em $(F_2, \mathcal{O}_2)$.

Se este tipo é realizável por algum $x_2 \in F_2$, então, lembrando a tradução em (104), vale evidentemente

$$v_2(x_2 - a) = v(b_a) = v_1(x_1 - a) \quad \text{para todo } a \in F.$$

Tomamos um subconjunto finito de $\Phi(z_0)$, ou seja, escolhemos $a_1, ..., a_n \in F$ com os respectivos $b_{a_1}, ..., b_{a_n}$ como visto acima. Procuramos um elemento $d \in F_2$ tal que

$$v_2(d - a_1) = v(b_{a_1}), ..., v_2(d - a_n) = v(b_{a_n}). \tag{112}$$

Seja

$$v(b_a) = \max_{1 \leq i \leq n} \{v(b_{a_i})\}.$$

Como $v_1(x_1 - a) = v(b_a)$, temos que

$$(x_1 - a)b_a^{-1} \in \mathcal{O}_1^{\times},$$

e portanto

$$\overline{0} \neq \overline{(x_1 - a)b_a^{-1}} \in \overline{F_1}.$$

Por hipótese $\overline{F} = \overline{F_1}$, e então existe um $c \in F$ com $\overline{c} = \overline{(x_1 - a)b_a^{-1}}$. Logo

$$0 < v_1\left(\frac{x_1 - a}{b_a} - c\right) = v_1\left(\frac{x_1 - (a + cb_a)}{b_a}\right).$$

Tomando $d = a + cb_a \in F$ segue que

$$v_1(x_1 - d) > v(b_a) \geq v(b_{a_i}) = v_1(x_1 - a_i)$$

para todo $i \in \{1, ..., n\}$. Em particular vale

$$v(d - a_i) = v_1((x_1 - a_i) - (x_1 - d)) = v_1(x_1 - a_i) = v(b_{a_i}),$$

o que prova (112). Isto prova, pelo Lema 4.10.5, que $\Phi(z_0)$ é um Tipo de $(F_2, \mathcal{O}_2)$ e portanto, pela sua κ^+ saturação, existe $x_2 \in F_2$ realizando $\Phi(z_0)$.

Afirmamos que x_2 é transcendente sobre F. De fato, ampliamos o tipo $\Phi(z_0)$ para

$$\Phi_1(z_0) = \Phi(z_0) \cup \{f(z_0) \neq 0 \mid f \in F[X] \text{ é irredutível e } \deg(f) > 1\}.$$

Com o Corolário 3.6.17 e com o Lema 3.5.17, a extensão canônica para a henselização de $F(x_1)$

$$a \mapsto a \text{ para } a \in F \quad \text{e} \quad x_1 \mapsto x_2$$

define um monomorfismo que preserva a valorização de $F(x_1)$ em F_2 juntamente com as propriedades $(i) - (iii)$. Isto contradiz novamente nossa maximalidade.

Assim finalmente $F = F_1$.

■

Para uma aplicação posterior destacamos a parte da imersão da prova acima.

Lema 5.1.4 *Sejam $(F_\nu, \mathcal{O}_\nu)$ corpos henselianos com subcorpos henselianos $(F'_\nu, \mathcal{O}'_\nu)$ para $\nu = 1, 2$. Seja*

$$\sigma' : (F'_1, \mathcal{O}'_1) \to (F'_2, \mathcal{O}'_2)$$

um isomorfismo de corpos valorizados e sejam

$$\sigma'_r : \overline{F'_1} \to \overline{F'_2} \quad e \quad \sigma'_g : \Gamma'_1 \to \Gamma'_2$$

os isomorfismos induzidos entre os respectivos corpos de resíduos e grupos de valores.

Se

- Γ_1' *é puro em* Γ_1.
- $\mathsf{car}(\overline{F_1}) = 0$.
- $(F_2, \mathcal{O}_2)$ *é* $\mathsf{card}(F_1)^+$*-saturada*
- σ_r' *e* σ_g' *estendem-se para imersões* σ_r *e* σ_g *de* $\overline{F_1}$ *em* $\overline{F_2}$ *e de* Γ_1 *em* Γ_2, *respectivamente.*

Então σ' *também se estende para uma imersão* σ *de* $(F_1, \mathcal{O}_1)$ *em* $(F_2, \mathcal{O}_2)$, *que induz* σ_r *e* σ_g.

Relembramos as traduções $\varphi \mapsto \varphi_r$ e $\varphi \mapsto \varphi_g$ que fizemos no início desta seção. Sejam Σ_r um sistema de axiomas para T_r (teoria de corpos) e Σ_g um sistema de axiomas para T_g (teoria de grupos abelianos ordenados). Pelo que vimos, um sistema de axiomas Σ para a teoria T de corpos valorizados henselianos pode ser tomado como:

1. $K_0 - K_9$
2. $V_1 - V_3$, H_n para $n \geq 2$
3. α_r para $\alpha \in \Sigma_r$
4. β_g para $\beta \in \Sigma_g$

O próximo teorema foi provado independentemente por Ax-Kochen e Ershov. Ele é o principal teorema da Teoria dos Modelos dos corpos Henselianos.

Teorema 5.1.5 *Sejam* $(F_1, \mathcal{O}_1)$ *e* $(F_2, \mathcal{O}_2)$ *corpos henselianos com corpos de resíduos* $\overline{F_1}$ *e* $\overline{F_2}$ *e grupos de valores* Γ_1 *e* Γ_2. *Se*

- $\mathsf{car}(\overline{F_1}) = 0$,
- $\overline{F_1} \equiv \overline{F_2}$ *na linguagem de corpos,*
- $\Gamma_1 \equiv \Gamma_2$ *na linguagem de grupos,*

então $(F_1, \mathcal{O}_1) \equiv (F_2, \mathcal{O}_2)$ *na linguagem de corpos valorizados.*

Prova. Pelo Teorema da Existência (Teorema 4.10.9), podemos supor que $(F_\nu, \mathcal{O}_\nu)$ é $\aleph_1$-saturada e que $\aleph_1 \leq \mathsf{card}(F_\nu)$, para $\nu \in \{1,2\}$. Como $\overline{F_1} \equiv \overline{F_2}$ e $\mathsf{car}(\overline{F_1}) = 0$, também temos que $\mathsf{car}(F_1) = \mathsf{car}(F_2) = 0$.

(Ressaltamos que passando para uma extensão elementar, ou uma subestrutura elementar, a equivalência dos grupos de valores e dos corpos de resíduos permanece, lembrando as traduções que fizemos no início do Capítulo.)

Vamos contruir agora, para cada $\nu \in \{1,2\}$, uma cadeia ascendente

$$(F_\nu^{(0)}, \mathcal{O}_\nu^{(0)}) \subset (F_\nu^{(1)}, \mathcal{O}_\nu^{(1)}) \subset \ldots \subset (F_\nu^{(n)}, \mathcal{O}_\nu^{(n)}) \subset \ldots \subset (F_\nu, \mathcal{O}_\nu),$$

onde $(F_\nu^{(n)}, \mathcal{O}_\nu^{(n)})$ é henseliano e enumerável para $\nu \in \{1,2\}$ para todo $n \in \mathbb{N}$. Também construímos os isomorfismos

$$\sigma^{(n)} : (F_1^{(n)}, \mathcal{O}_1^{(n)}) \to (F_2^{(n)}, \mathcal{O}_2^{(n)}),$$

tais que $\sigma^{(n+1)}$ é uma extensão de $\sigma^{(n)}$.

Mais ainda, a construção será tal que para todo $n \in \mathbb{N}$ com $n \geq 1$ valem:

(1) $(F_1^{(2n-1)}, \mathcal{O}_1^{(2n-1)}) \prec (F_1, \mathcal{O}_1)$.

(2) $(F_2^{(2n)}, \mathcal{O}_2^{(2n)}) \prec (F_2, \mathcal{O}_2)$.

E para todo $n \in \mathbb{N}$ valem:

(3) $(\overline{F_1}, (\overline{a})_{a \in \mathcal{O}_1^{(n)}}) \equiv (\overline{F_2}, (\overline{\sigma^{(n)}(a)})_{a \in \mathcal{O}_1^{(n)}})$.

(4) $(\Gamma_1, (v_1(a))_{a \in F_1^{(n)}}) \equiv (\Gamma_2, (v_2(\sigma^{(n)}(a)))_{a \in F_1^{(n)}})$.

Começamos nossa construção.

Construção da Cadeia:

- Para $n = 0$, como $\mathsf{car}(F_\nu) = 0$ para $\nu \in \{1,2\}$, temos que o menor subcorpo destes corpos é $\mathbb{Q}$. Definimos então

$$F_1^{(0)} := \mathbb{Q} =: F_2^{(0)}$$

e tomamos $\sigma^{(0)} = id_{\mathbb{Q}}$. Novamente pelo fato de $\mathsf{car}(\overline{F}) = 0$, temos pelo Teorema 3.3.28 que

$$\mathcal{O}_1^{(0)} = \mathcal{O}_2^{(0)} = \mathbb{Q}$$

para $\nu \in \{1, 2\}$. Em particular $(F_\nu^{(0)}, \mathcal{O}_\nu^{(0)})$ são henselianos para $\nu \in \{1, 2\}$.

Por fim temos que

$$\Gamma_1^{(0)} = \{0\} = \Gamma_2^{(0)}.$$

Neste caso temos trivialmente (1) e (2), e claramente (3) e (4). (Lembramos que estas condições são requisitas apenas para $n \geq 1$.)

- Para $n = 1$ procedemos da seginte forma: Pelo Teorema 4.8.8 existe uma subestrutura elementar enumerável $(F_1^{(1)}, \mathcal{O}_1^{(1)})$ de $(F_1, \mathcal{O}_1)$ que contêm $(F_1^{(0)}, \mathcal{O}_1^{(0)})$. Para tal $F_1^{(1)}$, também vale que o seu corpo de resíduos $\overline{F_1^{(1)}}$ e o seu grupo de valores $\Gamma_1^{(1)}$ são enumeráveis e que

$$\overline{F_1^{(1)}} \equiv \overline{F_1} \equiv \overline{F_2} \quad \text{e} \quad \Gamma_1^{(1)} \equiv \Gamma_1 \equiv \Gamma_2.$$

Por causa da $\aleph_1$-saturabilidade de $\overline{F_2}$ e Γ_2 (lembre do Lema 5.1.2), pelo Corolário 4.10.16 existem imersões elementares

$$\sigma_r^{(1)} : \overline{F_1^{(1)}} \to \overline{F_2} \quad \text{e} \quad \sigma_g^{(1)} : \Gamma_1^{(1)} \to \Gamma_2.$$

Como $\Gamma_1^{(0)} = \{0\}$ é puro em $\Gamma_1^{(1)}$, pelo Lema 5.1.4, a aplicação identidade $\sigma^{(0)} : (F_1^{(0)}, \mathcal{O}_1^{(0)}) \to (F_2^{(0)}, \mathcal{O}_2^{(0)})$ estende-se para um isomorfismo

$$\sigma^{(1)} : (F_1^{(1)}, \mathcal{O}_1^{(1)}) \to (F_2^{(1)}, \mathcal{O}_2^{(1)}) \subset (F_2, \mathcal{O}_2),$$

que induz isomorfismos nos corpos de restos e nos grupos de valores da seguinte forma:

$$\sigma_r^{(1)}(\overline{a}) = \overline{\sigma^{(1)}(a)} \quad \text{e} \quad \sigma_g^{(1)}(v_1(a)) = v_2(\sigma^{(1)}(a)).$$

Portanto, para $n \in \{0, 1\}$ temos garantidas as condições (3) e (4) e trivialmente (1) e (2).

- A passagem de $n = 1$ para $n = 2$ sinaliza como passaremos de n para $n+1$ no caso genérico. Para um n par definiremos um isomorfismo $\sigma^{(n+1)}$, enquanto que para um n ímpar definiremos um isomorfismo $(\sigma^{(n+1)})^{-1}$.

Agora neste caso concreto definimos $(\sigma^{(2)})^{-1}$.

No caso $n = 1$ definimos $\sigma^{(1)}$ de modo que valem (3) e (4), ou seja, em particular valem

$$(\overline{F_1}, (\alpha)_{\alpha \in \overline{F_1^{(1)}}}) \equiv (\overline{F_2}, (\sigma_r^{(1)}(\alpha))_{\alpha \in \overline{F_1^{(1)}}})$$

e

$$(\Gamma_1, (\gamma)_{\gamma \in \Gamma_1^{(1)}}) \equiv (\Gamma_2, (\sigma_g^{(1)}(\gamma))_{\gamma \in \Gamma_1^{(1)}}).$$

Com ajuda do Teorema 4.8.8 escolhemos $(F_2^{(2)}, \mathcal{O}_2^{(2)})$ como uma subestrutura elementar enumerável de $(F_2, \mathcal{O}_2)$ que contém $(F_2^{(1)}, \mathcal{O}_2^{(1)})$. Em particular também valem

$$(\overline{F_1}, (\alpha)_{\alpha \in \overline{F_1^{(1)}}}) \equiv (\overline{F_2^{(2)}}, (\sigma_r^{(1)}(\alpha))_{\alpha \in \overline{F_1^{(1)}}})$$

e

$$(\Gamma_1, (\gamma)_{\gamma \in \Gamma_1^{(1)}}) \equiv (\Gamma_2^{(2)}, (\sigma_g^{(1)}(\gamma))_{\gamma \in \Gamma_1^{(1)}}).$$

Pelo Corolário 4.10.16 existem imersões elementares

$$(\sigma_r^{(2)})^{-1} : \overline{F_2^{(2)}} \to \overline{F_1} \quad \text{e} \quad (\sigma_g^{(2)})^{-1} : \Gamma_2^{(2)} \to \Gamma_1,$$

que estendem $(\sigma_r^{(1)})^{-1}$ e $(\sigma_g^{(1)})^{-1}$.

Finalmente, como $\Gamma_2^{(1)} = \sigma_g^{(1)}(\Gamma_1^{(1)})$ é uma subestrutura elementar de Γ_2, também $\Gamma_2^{(1)}$ é puro em $\Gamma_2^{(2)}$.

Utilizando o Lema 5.1.4 obtemos uma extensão

$$(\sigma^{(2)})^{-1} : (F_2^{(2)}, \mathcal{O}_2^{(2)}) \to (F_1^{(2)}, \mathcal{O}_1^{(2)}) \subset (F_1, \mathcal{O}_1)$$

de $(\sigma^{(1)})^{-1}$, a qual induz $(\sigma_r^{(2)})^{-1}$ e $(\sigma_g^{(2)})^{-1}$.

Aplicamos esta construção iteradamente e obtemos o seguinte diagrama.

Novamente concluímos (1)-(4).

$$\begin{array}{ccc}
F_1 & & F_2 \\
| & & | \\
F_1' & \xrightarrow{\sigma' \ \sim} & F_2' \\
\vdots & & \vdots \\
F_1^{(2)} & \xleftarrow[(\sigma^{(2)})^{-1}]{} & F_2^{(2)} \\
| & & | \\
F_1^{(1)} & \xrightarrow{\sigma^{(1)}} & F_2^{(1)} \\
| & & | \\
F_1^{(0)} = \mathbb{Q} & \xrightarrow{id=\sigma^{(0)}} & \mathbb{Q} = F_2^{(0)}
\end{array}$$

Tomamos agora

$$F_1' = \bigcup_n F_1^{(n)} \ , \ F_2' = \bigcup_n F_2^{(n)} \ , \ \sigma' = \bigcup_n \sigma^{(n)}.$$

Obteremos a seguinte situação com o isomorfismo σ':

$$\begin{array}{ccc}
(F_1, \mathcal{O}_1) & & (F_2, \mathcal{O}_2) \\
| & & | \\
\sigma' : (F_1', \mathcal{O}_1') & \to & (F_2', \mathcal{O}_2')
\end{array}$$

Para $\nu \in \{1, 2\}$ temos

$$F_\nu' := \bigcup_n F_\nu^{(2n)} = \bigcup_n F_\nu^{(2n-1)}.$$

Pelas propriedades (1) e (2) e pelo Teorema 4.9.14 e Observação 4.9.15, para $\nu \in \{1, 2\}$, vale

$$(F_\nu', \mathcal{O}_\nu') \prec (F_\nu, \mathcal{O}_\nu).$$

Então, empregando o Teorema 4.10.17, já que $(F_1', \mathcal{O}_1')$ e $(F_2', \mathcal{O}_2')$ são isomorfas por σ' e são saturadas, elas são elementarmente equivalentes, e por fim,

$$(F_1, \mathcal{O}_1) \equiv (F_1', \mathcal{O}_1') \equiv (F_2', \mathcal{O}_2') \equiv (F_2, \mathcal{O}_2).$$

■

Definição 5.1.6 *Dados um corpo K e um inteiro positivo i, dizemos que K é um corpo $C_i(d)$ se todo polinômio homogêneo de grau total d em mais de d^i variáveis e com coeficientes em K admite uma solução não trivial em K. O corpo K é dito ainda um C_i-corpo se for $C_i(d)$ para todo $d \in \mathbb{N}^*$.*

Teorema 5.1.7 (Ax-Kochen, 1965) *Para cada grau d existe uma cota n_d tal que se $p \geq n_d$ então cada polinômio homogêneo de grau d em mais de d^2 indeterminadas sobre $\mathbb{Q}_p$ reproduz o zero de forma não trivial.*

Prova. Suponhamos que existe um grau d para o qual tal cota não existe. Então existe um subconjunto infinito B do conjunto dos números primos $\mathbb{P}$, a saber,

$$B = \{p \mid p \text{ é primo e } \mathbb{Q}_p \text{ não é } C_2\}$$

e claramente $\mathsf{card}(B) = \aleph_0$.

Temos assim para cada $p \in B$ um polinômio $f_p \in \mathbb{Q}_p[X_1, ..., X_m]$ homogêneo de grau d com mais do que d^2 variáveis e tal que

$$f_p(a_1, ..., a_m) = 0 \ \Rightarrow \ \forall i \ , \ a_i = 0$$

ou seja, só reproduz o zero de forma trivial.

Faremos agora algumas reduções para simplificar o problema.

Redução 1: Podemos supor que para todo $p \in B$ o polinômio f_p possui um termo αX_1^d com $\alpha \in \mathbb{Q}_p$ e $\alpha \neq 0$.

De fato, se f_p não possui um tal termo, então consideramos o polinômio

$$g_p(X_1, ..., X_m) := f_p(\alpha X_1, X_2 + \alpha X_1, ..., X_m + \alpha X_1); \qquad 0 \neq \alpha \in \mathbb{Q}_p.$$

Cada termo da forma $b_k X_1^{i_1} ... X_m^{i_m}$ de f_p é transformado num termo de g_p da forma

$$b_k(\alpha X_1)^{i_1}(X_2 + \alpha X_1)^{i_2} ... (X_m + \alpha X_1)^{i_m},$$

onde $i_1 + ... + i_m = d$, pois f_p é homogêneo de grau d. Disto segue que g_p possui um termo da forma

$$(\sum_k b_k \alpha^d) X_1^d = f_p(\alpha, ..., \alpha) X_1^d = c X_1^d$$

onde $c \neq 0$ pela escolha de f_p e por $\alpha \neq 0$. Na verdade c é o coeficiente de X_1^d em g_p.

Como fizemos uma mudança de variáveis linear (isomorfismo), g_p é homogêneo de grau d. Agora f_p representa o zero apenas trivialmente se, e somente se, g_p representa o zero apenas trivialmente. Isto segue de

$$\begin{aligned} g_p(\beta_1, ..., \beta_m) = 0 \ \Leftrightarrow \ & f_p(a_1, a_2, ..., a_m) \ = \ 0 \ ; \\ & \alpha\beta_1 = a_1 \ , \ \beta_j + \alpha\beta_1 = a_j; \ \forall \ 2 \leq j \leq m \end{aligned}$$

e então

$$\begin{aligned} a_1 = ... = a_m = 0 \ &\Leftrightarrow \ \alpha\beta_1 = 0 \ , \ \beta_j - \alpha\beta_1 = 0 \ , \ \forall \ 2 \leq j \leq m \\ &\Leftrightarrow \ \beta_1 = ... = \beta_m \ = \ 0. \end{aligned}$$

Redução 2: Podemos supor que todos os f_p envolvem apenas $d^2 + 1$ indeterminadas.

Por hipótese podemos supor que cada f_p envolve, efetivamente, $m \geq d^2 + 1$ das indeterminadas $X_1, ..., X_m$.

Para cada $i > d^2 + 1$ substituímos a indeterminada X_i por 0 e obtemos um polinômio homogêneo de grau d não nulo graças a *Redução 1*. Ele continua representando o zero apenas de forma trivial. De fato, se este reproduz o zero de forma não trivial, ou seja existe $(\alpha_1, ..., \alpha_{d^2+1}) \neq (0, ..., 0)$ com

$$f(\alpha_1, ..., \alpha_{d^2+1}, 0, ..., 0) = 0,$$

chegamos numa contradição.

Portanto, pela *Redução 1* e *Redução 2* podemos supor que

$$f_p \in \mathbb{Q}_p[X_1, ..., X_{d^2+1}]$$

e que envolve efetivamente X_1^d.

Agora denotaremos por

$$f(Y_1, ..., Y_t, X_1, ..., X_{d^2+1})$$

o polinômio genérico nas variáveis $X_1, ..., X_{d^2+1}$ com coeficientes $Y_1, ..., Y_t$. Então, vale em todo $\mathbb{Q}_p$ com $p \in B$, a seguinte sentença elementar φ da linguagem de corpos:

$$\exists\, Y_1, ..., Y_t \quad \left[\bigvee_{i=1}^{t} Y_i \neq 0 \ \wedge\ \forall\, X_1, ..., X_n \right.$$
$$\left. \left(f(Y_1, ..., Y_t, X_1, ..., X_n) \doteq 0 \ \Rightarrow\ \bigwedge_{j=1}^{n} X_j \doteq 0 \right) \right],$$

onde $n = d^2 + 1$ está fixado.

Ou seja, para todo $p \in B$,

$$\mathbb{Q}_p \models \varphi.$$

Seja $\mathcal{F}_0$ o filtro dos conjuntos cofinitos de $\mathbb{P}$:

$$\mathcal{F}_0 = \{ A \subset \mathbb{P} \mid \mathbb{P} - A \ \text{ é finito } \}.$$

É evidente que

$$\mathcal{F}_0 \cup \{ U \cap B \mid U \in \mathcal{F}_0 \}$$

é um conjunto de conjuntos não vazios de $\mathbb{P}$ que é fechado para interseção. Pelo Lema 4.11.6 podemos estender este conjunto para um ultrafiltro $\mathcal{F}$ de $\mathbb{P}$. Como $\mathcal{F}_0$ é um filtro vale $\mathbb{P} \in \mathcal{F}_0$, e logo $\mathbb{P} \cap B = B \in \mathcal{F}$.

Como $B \in \mathcal{F}$, pelo Teorema de Los 4.11.12 a sentença α vale também no ultraproduto

$$F_1 = \prod_{p \in \mathbb{P}} \mathbb{Q}_p \ / \ \mathcal{F}$$

Por outro lado, como antes mencionamos (ver [8]), sabemos que o corpo $\mathbb{F}_p((t))$ é C_2. Em particular, como $\mathbb{P} \in \mathcal{F}$, vale $\neg\varphi$ no ultraproduto

$$F_2 = \prod_{p\in\mathbb{P}} \mathbb{F}_p((t)) \ / \ \mathcal{F}$$

Veremos agora que F_1 e F_2 são elementarmente equivalentes. Assim a nossa hipótese de não existência de uma cota n_d nos levará a uma contradição.

A fim de verificarmos que $F_1 \equiv F_2$, construímos o ultraproduto dos corpos acima considerados junto com seus anéis de valorização canônicos,

$$(F_1, \mathcal{O}_1) = \prod_{p\in\mathbb{P}} (\mathbb{Q}_p, \mathbb{Z}_p) \ / \ \mathcal{F} \quad \text{e} \quad (F_2, \mathcal{O}_2) = \prod_{p\in\mathbb{P}} (\mathbb{F}_p((t)), \mathbb{F}_p[[t]]) \ / \ \mathcal{F}.$$

O grupo de valores e o corpo de resíduos dos corpos valorizados acima são, para ambos, os respectivos Ultraprodutos

$$\prod_{p\in\mathbb{P}} \mathbb{Z} \ / \ \mathcal{F} = \mathbb{Z}^{\mathbb{P}} \ / \ \mathcal{F} \quad \text{e} \quad \prod_{p\in\mathbb{P}} \mathbb{F}_p \ / \ \mathcal{F}.$$

Para cada $p \in \mathbb{P}$ a sentença sobre a característica

$$C_p \ : \ \underbrace{1 + \ldots + 1}_{p \text{ vezes}} \doteq 0$$

vale no fator $\mathbb{F}_q$ se, e somente se, $p = q$. Então pelo Teorema de Los (Teorema 4.11.12), C_p vale no corpo de resíduos somente se $\{p\} \in \mathcal{F}$. Isto não ocorre pois o nosso filtro é não principal.

Logo a característica do corpo de resíduos é zero. Com isto, segue do Teorema 5.1.5 a equivalência elementar de $(F_1, \mathcal{O}_1)$ e $(F_2, \mathcal{O}_2)$, e em particular de $F_1 \equiv F_2$.

■

Índice Remissivo

Referências

[1] Ax,J.-Kochen,S., *Diophantine problems over local fields, I+II,* Am. J. Math. 87 (1965) 605-648.

[2] Chevalley,C., *Démonstration d'une hypothèse de M.Artin,* Abh.Math. Sem. Univ. Hamburg 11 (1936) 73-75.

[3] Delzell,C. - Prestel, A., *Positive Polynomials,* Springer Monographs in Mathematics, Srpinger-Verlag, 2001.

[4] Engler,A.J. - Prestel,A., *Valued Fields,* Springer Monographs in Mathematics, Srpinger-Verlag, 2005.

[5] Friedrichsdorf, U. - Prestel,A., *Mengenlehre für den Mathemtiker,* Grundkurs Mathematik, Vieweg, 1985.

[6] Garcia,A. - Lequain,Y., *Elementos de Álgebra,* Projeto Euclides, IMPA, 2002.

[7] Lang,S., *Algebra,* Addison_Wesley,1972

[8] Lang,S., *On quasi algebraic closure,* Annals of Math. 55 (1963) 378-391.

[9] Lewis,D.J., *Cubic homogeneous polynomials over $p-adic$ fields,* Annals of Math. 56 (1952) 473-478.

[10] Morandi,P., *Field and Galois Theory,* New York, Springer, 1996.

[11] Prestel, A., *Einführung in die Mathematische Logik und Modelltheorie,* Aufbaukurs Mathematik, Vieweg, 1986.

[12] Ribenboim, P., *The Theory of Classical Valuations,* Springer Monographs in Mathematics, Srpinger-Verlag, 1998.

[13] Terjanian,G., *Un contre-example à une conjecture d 'Artin.* C. R. Acad. Sci. Paris 262 (1966) 612.