UNIVERSIDADE FEDERAL DO CEARÁ

Classificação de Alguns Corpos de Gênero Zero

JOSÉ GOMES DE ASSIS

MONOGRAFIA SUBMETIDA À COORDENAÇÃO DO
CURSO DE PÓS - GRADUAÇÃO EM MATEMÁTICA
PARA OBTENÇÃO DO GRAU DE MESTRE

FORTALEZA - 1989

CLASSIFICAÇÃO DE ALGUNS CORPOS DE GÊNERO ZERO

JOSÉ GOMES DE ASSIS

DISSERTAÇÃO SUBMETIDA À COORDENAÇÃO DO
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA, COMO REQUISITO
PARCIAL PARA OBTENÇÃO DO GRAU DE MESTRE
UNIVERSIDADE FEDERAL DO CEARÁ

FORTALEZA - 1989

Í N D I C E

D E D I C A T Ó R I A

A minha esposa *Fátima* e as minhas filhas, *Cibelle, Thaís* e *Priscilla*.

A G R A D E C I M E N T O S

Agradeço ao Professor *Hermínio Borges Neto* pela orientação dada durante todo o meu Curso de Mestrado, especialmente na elaboração desta monografia.

Sou grato em especial a minha esposa pelo modo que suportou e administrou o meu afastamento do convívio doméstico durante o período que passei no Ceará.

Agradeço ao Professor *João Montenegro de Miranda* pelas sugestões dada numa primeira versão deste trabalho.

Sou grato aos colegas do Departamento de Matemática da Universidade Federal da Paraíba que me possibilitaram vir para a Universidade Federal do Ceará.

Agradeço a Universidade Federal do Ceará, em particular à Coordenação de Pós-Graduação em Matemática, pelos recursos postos ao meu dispor. Também sou grato a CAPES pelo suporte financeiro durante o curso de mestrado.

Finalmente, agradeço a *Regina Fátima Alves* pelo trabalho de datilografia.

I N T R O D U Ç Ã O

Este trabalho, baseado em notas não publicadas do Professor Herminio Borges de Neto, |N|, estudamos Corpos de Funções Algébricas de uma variável com gênero zero.

No Capítulo I estudamos os fundamentos da Teoria das valorizações e dos corpos reais, mais precisamente as trocas de Artin-Schreier e Kummer. Já no Capítulo II estudamos o teorema de Riemann-Roch, para corpos de funções algébricas, o qual será fundamental para a determinação do gênero, e para se caracterizar os corpos de gênero zero em termos de equações algébricas entre geradores.

Finalmente no Capítulo III, caracterizamos os Corpos de Funções de gênero zero nos casos em que k é finito e no caso em que o grau do fecho algébrico de k sobre k é finito.

1 - CONCEITOS BÁSICOS

1.1. - Preliminares

k representa um corpo arbitrário fixo com $1 \neq 0$.

Seja $E|k$ uma extensão de corpos e $S \subset E$. Lembramos que S é chamado um subconjunto algebricamente independente sobre k, se $k[S]$ é naturalmente k-isomorfo ao anel de polinômios $k[T]$, onde T é um conjunto de indeterminados sobre k, com mesma cardinalidade que S, isto é, dados $f(t_1,t_2,\ldots,t_n) \in k[T]$ e $x_1,x_2,\ldots,x_n \in S$ com $f(x_1,x_2,\ldots,x_n) = 0$ temos $f = 0$. Caso contrário diz-se que S é algebricamente dependente sobre k. Um conjunto algebricamente independente maximal é chamado uma base de transcedência de $E|k$. Pode-se provar (veja [L], Cap.X) que duas bases de transcedância de $E|k$ têm mesma cardinalidade; essa cardinalidade comum é chamada o grau de transcedência de $E|k$.

Se $E' = k(S)$, corpo quociente de $k[S]$ em E, S base de transcendência, tem-se $E'|E$ algébrica; se $E = E'$ diz-se que $E|k$ é transcendente pura. A extensão $E|k$ é dita finitamente gerada ou de tipo finito se $E = k(S)$, e S é um conjunto finito; nesse caso, se existe uma base de transcedência S' de $E|k$ tal que $E|k(S')$ é algebricamente separável diz-se que se trata de uma extensão separavelmente gerada.

1.2. - Valorizações

1.1.2. Definição

Seja E um corpo. Uma valorização (de posto 1) de E é uma aplicação

$$v: E \to \mathbb{R} \cup \{\infty\} \qquad (\mathbb{R} \text{ é o corpo dos reais})$$

tal que:

(i) $v(x.y) = v(x) + v(y) \quad \forall\, x,y \in E$

(ii) $v(x+y) \geq \min\{v(x), v(y)\} \quad \forall\, x,y \in E^*$

(iii) $v(x) = \infty$ se, somente se, $x = 0$.

O conjunto de valores $\{v(x);\ x \in E,\ x \neq 0\}$ é um subgrupo de $\mathbb{R}$, que é chamado de Grupo de Valores de v, que denotamos por $v(E^*)$.

Convencionamos que:

(1) $\infty + n = \infty$, para cada n em $\mathbb{R}$

(2) $\infty + \infty = \infty$

(3) $n < \infty$, para cada $n \in \mathbb{R}$.

Para uma valorização v, são verificadas as seguintes propriedades:

(1) $v(\pm 1) = 0$

(2) $v(x^{-1}) = -v(x) \quad \forall\, x \in E^*$

(3) $v(-x) = v(x) \quad \forall\, x \in E$

Uma valorização v diz-se discreta, se o grupo de valores $v(E^*)$ é discreta, isto é; $v(E^*) = \mathbb{Z}.r$, onde r é um número real positivo. v é normalizada, se $v(E^*) = \mathbb{Z}$.

Se E é uma extensão do corpo K e v uma valorização de E, então a restrição de v à K define uma valorização de K. No caso de $v(x) = 0$ para todo $x \in K^*$ dizemos que v é <u>trivial sobre K</u> e <u>v é uma valorização de E sobre K.</u>

Exemplos:

(1) Seja $p(x)$ e $k[x]$ irredutível sobre k.

Definimos a aplicação $v_p: k[x] \to \mathbb{Z} \cup \{\infty\}$ da seguinte forma

$$v_p(f) = \begin{cases} \infty, \text{ se } f = 0 \\ \text{Expoente de } p(x) \text{ na decomposição de } f(x) \text{ em fatores irredutíveis, se } f \neq 0. \end{cases}$$

Estendendo esta definição para o corpo de funções racionais $k(x)$ de $k[x]$, por $v_p(f/g) = v_p(f) - v_p(g)$. Desta forma v_p é uma valorização de $k(x)$ sobre k, chamada a <u>valorização p(x) - ádica de k(x) sobre k</u>.

(2) Ainda sobre $k[x]$ definimos a função $v_\infty: k[x]^* \to \mathbb{Z}$ como

$v_\infty(f) = -\text{grau de } f = -\partial f$.

Da mesma forma, estendemos v_∞ para $k(x)$ por, $v_\infty(f/g) = v_\infty(f) - v_\infty(g) = \partial g - \partial f$. Assim v_∞ é uma valorização de $k(x)$ sobre k, chamada <u>valorização infinita de k(x) sobre k.</u>

1.2.2. - <u>Lema</u>

Sejam E um corpo e $x_1, x_2, \ldots, x_n$ pertencentes a E e v uma valorização de E. Então:

(1) $v(x_1 + x_2 + \ldots + x_n) \geq \min \{v(x_1), v(x_2), \ldots, v(x_n)\}$

(2) Se o mínimo é assumido uma única vez, então

$v(x_1 + x_2 + \ldots + x_n) = \min\{v(x_1), v(x_2), \ldots, v(x_n)\}$

Demonstração: Veja, [0]

1.2.3. - Proposição

Seja v uma valorização de E. O conjunto

$$A_v = \{x \in E;\ v(x) \geq 0\}$$

é um sub-anel de E, denominado anel de valorização de v sobre E, tendo $m_v = \{x \in E;\ v(x) > 0\}$ o seu único ideal maximal.

Além do mais, dado $x \in E^*$, x ou x^{-1} pertence a A_v:

Demonstração: Veja [E] capítulo II.

É fácil ver que, $x \in A_v$ é unidade se, somente se $v(x) = 0$. O conjunto $U = \{x \in E^*;\ v(x) = 0\}$ chamamos grupo das unidades de A_v.

Dizemos que duas valorizes v e ω de K são equivalentes se existe $\lambda > 0$, tal que $v(x) = \lambda\omega(x)\ \forall\ x \in K$.

Observemos que se v e v' são equivalentes então elas têm o mesmo anel de valorização.

1.2.4. - Proposição

Se duas valorizações v e v' de E têm o mesmo anel de

valorização, então elas são equivalentes.

Demonstração: Como $A = A_v = A_\omega$, então $\forall_x \in A$, $v(x) \geqslant 0$ se, somente se, $\omega(x) \geqslant 0$.

Consideremos v a valorização não trivial, então existe $z \in E$ tal que $v(z) < 0$, assim $v(z) \ngeqslant 0$ e $\omega(z) \ngeqslant 0$ portanto $\omega(z) < 0$ também.

Para todo $m, n \in \mathbb{Z}$ com $n>0$ e para algum x não nulo de E temos

$$\frac{m}{n} \geqslant \frac{v(x)}{v(z)} \Leftrightarrow mv(z) \geqslant nv(x) \Leftrightarrow v(z^m) \geqslant v(x^n) \Leftrightarrow$$

$$v(z^m) - v(x^n) \geqslant 0 \Leftrightarrow v(z^m/x^n) \geqslant 0 \Leftrightarrow \omega(z^m/x^n) \geqslant 0$$

$$\omega(z^m) - \omega(x^n) \geqslant 0 \Leftrightarrow m\omega(z) \geqslant n\omega(x) \Leftrightarrow$$

$$\frac{m}{n} \geqslant \frac{\omega(x)}{\omega(z)}$$

temos assim que $\forall m,n \in \mathbb{Z}$, $n > 0$ $n \neq 0$, $\in E$

$$\frac{m}{n} \geqslant \frac{v(x)}{v(z)} \Leftrightarrow \frac{m}{n} \geqslant \frac{\omega(x)}{\omega(z)} \quad \text{logo} \quad \frac{\omega(x)}{\omega(z)} = \frac{v(x)}{v(z)}$$

daí $v(x) = \dfrac{v(z)}{\omega(z)} \cdot \omega(x)$. $\forall x \in E$.

Seja $\lambda = \dfrac{v(z)}{\omega(z)} > 0$ daí $v(x) = \lambda\omega(x)$ $\forall x \in E$

isto é, v é equivalente a ω.

1.2.5. - Definição

Sejam E uma extensão do corpo k e v uma valorização de E. Define-se o corpo de resíduos de v como sendo o quociente. $E_v = A_v/M_v$.

Exemplos: Consideremos $E = k(x)$, sendo x transcendente sobre k, e v uma valorização de $E|k$ e $f/g \in E$ escrito na sua forma irredutível.

(1) Se v é trivial então, $M_v = (0)$ e $E_v \simeq k(x)$

(2) Se v é a valorização infinita então

$A_v = \{f|g;\ \partial g \geqslant \partial f\}$ e $M_v = \{f|g;\ \partial g > \partial f\}$

Portanto $E_v = \{f|g + M_v;\ \partial g \geqslant \partial f\}$.

Sejam $f(x) = a_o + a_1x + \ldots + a_nX^n$ e

$g(x) = b_o + b_1x + \ldots + b_mX^n$

$$\frac{f}{g} = \left[\frac{a_n}{b_n}(b_nX^n + \sum_{k=1}^{n-1} b_kX^k) - \sum_{k=1}^{n-1}\frac{a_n}{b_n}b_kX^k + \sum_{k=1}^{n-1} q_kX^k\right]/g$$

$$\frac{f}{g} = \frac{a_n}{b_n} - \left[\sum_{k=1}^{n-1}\left(\frac{a_n}{b_n}b_kX^k - a_k\right)X^k\right]/g \text{ . Assim}$$

$$\left(\overline{\frac{f}{g}}\right) = \frac{\overline{a_n}}{\overline{b_n}}$$. Deste modo, vemos, trivialmente, que $E_v \simeq k$.

(3) Se v é a valorização p(x) - ádica, então

$A_v = \{f/g; p \nmid g\}$ e $M_v = \{f/g;\ p \mid f$ e $p \nmid g\}$

Portanto, $E_v = \{f|g + M_v;\ f|g \in A_v\}$.

Consideremos Φ: $A_v \longrightarrow \frac{k[x]}{(p(x))}$

$$f|g \longrightarrow \overline{f} \cdot \overline{g}^{-1}$$

Φ é bem definido, pois se, $(f/g) = h/\ell)$ com $p\nmid g$ e $p|h$ temos, $(f\ell - hg)/g\ell = 0$ $\quad f\ell = hg \quad \overline{f}.\overline{\ell} = \overline{h}.\overline{g}$. Daí $\overline{f}.\overline{g}^{-1} = \overline{h}.\overline{\ell}^{-1}$. Φ é um homomorfismo sobrejetor com núcleo M_v. Pelo Teorema Fundamental dos Homomorfismos E_v é isomorfo a $k[x]/(p)$. Assim E_v é uma extensão algébrica finita de k, $E_v = k(\alpha)$, α raiz de $p(x)$, α pertencente ao fécho algébrico de k.

1.2.6. - Proposição

Sejam $E = k(x)$ um corpo de funções racionais sobre k e v uma valorização de E sobre k. Então, ou v é trivial ou v é equivalente a valorização p(x)-ádica para um polinômio irredutível p(x) em $k[x]$, ou v é equivalente a valorização infinita.

Demonstração:

Vamos supor que v é não trivial. Se $v(x) < 0$, afirmamos que v é equivalente a valorização infinita, v_∞.

De fato, se $f(x) = a_o + a_1X + \ldots + a_nX^n$, $a_n \neq 0$, então $v(f(x)) \geq \min_{0\leq i\leq n} \{iv(x)\} = nv(x)$ e sendo $v(a_iX^i)$ todos distintos, temos $v(f(x)) = nv(x)$.

Notemos que $v(f(x) = (-v(x)(-n) = \lambda v_\infty(f(x))$, onde $\lambda = -v(x) > 0$. Portanto v e v_∞ diferem em $k[x]$ por um fator positivo.

Em $k(x)$ temos $v(f|g) = v(f) - v(g) = \lambda v_\infty(f) - \lambda v_\infty(g) = \lambda v_\infty(f|g)$. Isto é, v e v_∞ diferem em $k(x)$ pelo mesmo fator positivo λ. Logo v é equivalente a v_∞.

Se $v(x) \geqslant 0$, seja $P_v = M_v \cap k[x]$. Afirmamos que $P_v \neq (0)$.

De fato, como $v(x) \geqslant 0$ temos $k[x] \subset A_v$, isto é $v(f) \geqslant 0 \quad \forall\, f \in k[x]$. Se $P_v = (0)$ então $v(f) = 0 \quad f \in k[x]$, e portanto v seria trivial. Logo $P_v \neq (0)$.

Como $k[x] \subset A_v$ e M_v é maximal em A_v, temos que P_v é maximal em $k[x]$ e portanto $P_v = (p(x))$ para algum $p(x)$ irredutível em $k[x]$.

Afirmamos que v é equivalente a valorização $p(x)$-ádica.

Para provarmos este fato vamos provar que os anéis das valorizações v e v_p coincidem.

Sejam A_v e A_{v_p} anéis de valorização de v e v_p respectivamente.

Seja $f/g \in A_{v_p}$, com $(f,g) = 1$.
Como $p \nmid g$ temos que $g \notin P_v$. Mas $v(g) \geqslant 0$, pois $v(x) \geqslant 0$ e assim $v(g) = 0$. Logo $f/g = f.1/g \in A_v$, isto é $A_{v_p} \subset A_v$.

Reciprocamente, consideremos $f/g \in A_v$ com $(f,g) = 1$ e suponhamos que $p|g$. Então $p \nmid f$, e assim $v(f) = 0$, isto é $f \notin M_v$. Como $p \nmid g$ temos que $g \in P_v$ e consequentemente $v(g) > 0$. Assim $v(f\,g) = v(f) - v(g) < 0$, o que é um absurdo, pois f pois $f/g \in A_v$. Então $p \nmid g$, logo $A_v \subset A_{v_p}$.

∎

1.2.7. - Definição

O grau de uma valorização v é o grau de E_v sobre k

e será denotado por d(v).

Observemos que em k(x) a valorização inffnita v_∞ tem grau 1..

1.2.8. - Teorema

Sejam K um corpo e B um subanel local de K. Então existe um anel de valorização A_v de K tal que B A_v e $M = B \cap M_v$ onde M é o ideal maximal de B e M_v o ideal maximal de A_v.

Demonstração: Veja [L] Capítulo IX § 1, proposição 9. ∎

1.2.9. - Teorema (Krull)

Sejam E um corpo e K um subcorpo de E.

Toda valorização v de K admite ao menos uma extensão a uma valorização ω de E.

Notemos se [E:K] é finito, então o número de extensões é finito.

Demonstração: Veja [L], Capítulo XII, § 4, Teorema 1. ∎

1.2.10. - Lema

Sejam E uma extensão algébrica do corpo K e v uma valorização não-trivial de E. Então v é não-trivial sobre k, isto é $v(K^*) \neq \{0\}$.

Demonstração:

Suponhamos, por absurdo, que existe uma valorização ω de E que é trivial sobre K. Seja $y \in E$ tal que $\omega(y) < 0$. Como y é algébrico sobre K, existem $c_1, c_2, \ldots, c_n$ nem todos nulos $\in K$ tal que $y^n + c_1 y^{n-1} + \ldots + c_{n-1} y + c_n = 0$. Como ω é trivial sobre K, vale $\omega(c_i) = 0$ ou ∞, para cada i, $i = 1, \ldots, n$. Logo $\omega(y^n) < \omega(c_i y^{n-1})$ para $i = 1, \ldots, m$ e $\infty = \omega(0) = \omega(y^n + \ldots + c_n) = n\omega(y) < 0$, absurdo. Logo $\omega(K^*) \neq \{0\}$. ∎

1.2.11. - Proposição

Sejam K um corpo e E uma extensão algébrica finita de K. Sejam v uma valorização de K e v' uma extensão de v a E. Então:

(1) v é trivial se, somente se, v' é trivial.

(2) v é discreta (de ponto 1) se, e somente se, v' é discreta (de ponto 1).

Demonstração : (Veja Valuation Theory, O. Endtee Cap. II). ∎

Sejam E uma extensão algébrica finita do corpo K e v uma valorização de K e v_i os prolongamentos de v à E. Como $v(K^*)$ é um subgrupo de $v_i(E^*)$ para cada i, chamamos $(V_i(E^*) : v(K^*)$ de Índice de Ramificação de v_i à E, que denotamos por ε_i.

Considerando $E|K$ uma extensão algébrica finita de K e ω uma valorização de E e $v = \omega_{|K}$, temos que A_v A_ω e $M_v = M \cap A_v$.

Logo temos uma imersão canônica

$$\pi;\ K_v \to E_\omega$$

$$x + A_v \to x + M_\omega$$

na qual identificamos $K_v \quad E_\omega$. Chamamos $|\ E_\omega : K_v\ |$ de índice de Inércia de ω à K, e denotamos por $f_{\omega|v}$.

1.2.12. - Teorema - Desigualdade Fundamental

Sejam E uma extensão algébrica finita de um corpo K, v uma valorização discreta de K com posto finito e $\omega_1, \omega_2, .. \omega_m$ as valorizações discretas de E inequivalentes entre si que prolongam v a E. Se $e_1, e_2, \ldots, e_n$ são os índices de ramificação de $\omega_1, \omega_2, \ldots, \omega_m$ a v e $f_1, f_2, \ldots, f_m$ seus respectivos índices de inércia, temos

$$e_1 f_1 + \ldots + e_n f_n < |E:K|.$$

Demonstração: Veja $|Z,S|_2$. Cap. VI, § 11, Teorema 19.

1.3. - Teorema de Artin-Schreier

Neste trabalho faremos uso de um teorema clássico da teoria dos corpos reais, o Teorema de Artin-Schreier. Para tanto faremos uma breve apresentação do que será necessário desta teoria.

1.3.1. - Definição

Seja K um corpo. Uma ordem de K é um subgrupo P de K^* tal que:

(1) Dado $x \in K$ temos que ou $x \in P$ ou $-x \in P$ ou $x = 0$ onde ou é, exclusivo.

(2) Se x e $y \in P$, então $x + y \in P$ e $x.y \in P$

P é também chamado de conjunto de elemento positivos de K e dizemos que K é ordenado por P.

1.3.2. - Proposição

Seja K um corpo ordenado por P. Então:

(1) 1 e $x^{-1} \in P$, $\forall\, x \in P$

(2) A característica de K é zero.

(3) $x^2 \in P \quad \forall\, x \in P$ e portanto $\sum_i x_i^2 \in P$ a não ser se todo $x_i = 0$.

Demonstração:

(1) Como $1 \neq 0$ temos que $1 \in P$ ou $-1 \in P$. Mas $1 = 1^2 = (-1)^2$. Logo $1 \in P$. Segue que $-1 \notin P$.

Suponhamos que $x \in P$ mas $x^{-1} \notin P$. Neste caso, $-x^{-1} \in P$. Assim $x.(-x^{-1}) = -1 \in P$ o que é um absurdo, pois $-1 \in P$. Logo $x^{-1} \in P \quad x \in P$.

(2) Pela definição de ordem de K e como $1 \neq 0$ temos que

$n.1 = 1+1...+1 \in P$, isto é $n.1 \neq 0 \quad n \in N$

Logo, K tem característica zero.

(3) Como $x \in K$ e $x \neq 0$ temos que $x \in P$ ou $-x \in P$ e portanto x^2 é positivo. Assim $\sum_i x_i^2 \in P$ a não ser se todo $x_i = 0$. ∎

Observemos que o produto de somas de quadrados em K é também soma de quadrados e se $x,g \in K$, são somas de quadrados com $y \neq 0$, então x/y é soma de quadrados pois, $(x/g) = x.y(y^{-1})^2$.

Concluimos assim, que o conjunto de somas de quadrados em K está contido em toda ordem de K.

1.3.3. - Proposição

Sejam P_1 e P_2 duas ordens de um corpo K. Então $P_1 \subset P_2$ implica $P_1 = P_2$.

Demonstração

Suponhamos $P_1 \neq P_2$ e seja $x \in P_2 - P_1$. Então $-x \in P_1 \subset P_2$, o que é uma contradição. Logo $P_1 = P_2$. ∎

Um corpo K é dito real se -1 não é soma de quadrados em K. O corpo dos reais (R) é um corpo real enquanto os complexos (C) não é real.

Um corpo K é dito real fechado, se for real e se não possui extensão algébrica que seja real. O corpo dos reais é real fechado.

1.3.4. - Proposição

Seja K um corpo real.

(1) Se $x \in K$, então $K(\sqrt{x})$ é real ou $K(\sqrt{-x})$ é real. Se x é soma de quadrados em K, então $K(\sqrt{x})$ é real. Se $K(\sqrt{x})$ é não real então -x é soma de quadrados em K.

(2) Se f é um polinômio irredutível de grau ímpar em $K[x]$ e α uma raiz de f, então $K(\alpha)$ é real.

Demonstração

(1) Seja $x \in K$. Se x é um quadrado em K, então $K = K(\sqrt{x})$ e $K(\sqrt{x})$ é real.

Vamos supor que x não é quadrado em K. Se $K(\sqrt{x})$ é não real, então existem b_i e $c_i \in K$ tais que

$$-1 = \sum_i (b_i + c_i\sqrt{x})^2 = \sum_i (b_i^2 + 2b_i c_i \sqrt{x} + c_i^2 x)$$

Como $\sqrt{x} \notin K$ e como $-1 \in K$ temos $2b_i c_i \sqrt{x} = 0$, logo $-1 = \sum_i b_i^2 + x\sum_i c_i^2$.

Se x é soma de quadrados em K, temos uma contradição. Portanto concluimos que

$$-x = \frac{1 + \sum_i b_i^2}{\sum_i c_i^2}$$

é soma de quadrados. Portanto $K(\sqrt{-x})$ é real, e assim provamos

a primeira afirmação.

(2) Provaremos a segunda afirmação usando indução finita sobre o grau de f.

(i) Se o grau de f é 1 então $f(x) = ax+b$, $a, b \in K$ e se $\alpha = -b/a \in K$, $K(\alpha) = K$ que é real.

(ii) Suponhamos a afirmação verdadeira para todo polinômio p de $K[x]$, irredutível de grau ímpar tal que $\partial p < \partial f$.

Suponhamos que $K(\alpha)$ não é real, então podemos escrever $-1 = \sum_i g_i(\alpha)^2$ com $g_i \in K[x]$, $\partial g_i \leq \partial f-1$.

Como $f(x) = irr(\alpha,K)$, temos que $f(x)$ divide $\sum_i g_i(x)^2 + 1$. Logo existe $h \in K[x]$ tal que

$$(*) \quad -1 = \sum_i g_i(x)^2 + h(x).f(x)$$

O polinômio $\sum_i g_i^2(x)$ tem grau par e maior do que zero, pois caso contrário -1 seria soma de quadrados em K; e esse grau é menor ou igual a $2(\partial f-1)$. Daí, ∂h é ímpar e menor ou igual a n-2. Portanto $\partial h < \partial f$. Sem perda de generalidades, vamos considerar h irredutível sobre K.

Se β é uma raiz de h, pela equação (*), temos que

$$-1 = \sum_i g_i(\beta)^2.$$

Isto é, -1 é soma de quadrados em $K(\beta)$. Logo $K(\beta)$ é não real, o que contradiz a hipótese de indução. Concluimos assim que $K(\alpha)$ é real.

■

1.3.5. - Definição

Seja K um corpo real. O fecho algébrico real de K, é um corpo R que é real fechado contendo K e tal que $R|K$ é algébrica.

Exemplo: Seja $\mathbb{Q}$ o corpo dos racionais e $\overline{\mathbb{Q}}$ seu fecho algébrico. O corpo $\mathbb{R} \cap \overline{\mathbb{Q}}$ é o fecho real de $\mathbb{Q}$.

1.3.6. - Teorema (Artin-Schreier) - Seja K um corpo real. Então

(1) Existe um único fecho real de K.

(2) Se R é um fecho real de K, então R tem uma única ordem, cujos elementos positivos são quadrados em R.

(3) Todo elemento positivo é quadrado e todo polinômio irredutível de grau ímpar em $R[x]$ tem raiz em R. Temos assim $\overline{R} = R(\sqrt{-1})$.

Demonstração: Veja [P] § 3, teorema 3.3. ∎

1.4. - Teoria de Kummer

Apresentaremos agora uma breve exposição da teoria de Kummer.

Sejam k um corpo e $\underline{m}$ um inteiro positivo. Uma extensão Galosiana K de k com grupo de Galois G é dita de expoente

$\underline{m}$ se $\sigma^m = 1$, $\sigma \in G$.

Vamos investigar as extensões cujo grupo de Galois é abeliano de expoente m. Assumiremos que m é um número primo com a característica de k e que k contém as raízes m-ésimas primitivas da unidade.

Denotaremos por $\mathbb{Z}_m$ o grupo das raízes m-ésimas da unidade e assumiremos que toda extensão algébrica de k está contida em seu fecho algébrico $\bar{k}$ de k.

Seja $a \in K$. Embora o símbolo $a^{1/m}$ não esteje bem definido, pois se $\alpha^m = a$ e ξ é uma raíz n-ésima da unidade, então também $(\xi\alpha)^m = a$, Assim vamos usar o símbolo $a^{1/m}$ para denotar algum tal elemento α, o qual será chamado de uma raíz m-ésima de a.

Como as raízes da unidades estão no corpo k observamos que o corpo $k(\alpha)$ é sempre o mesmo, não importando a m-ésima raiz dede a que escolhamos. Denotamos o corpo das m-ésimas raízes de a por $k(a^{1/m})$.

Sejam $k^{*m} = \{x^m;\ x \in k,\ x \neq 0\}$ e B um subgrupo de k^* contendo k^{*m}.

Vamos denotar por $k(B^{1/m})$ ou K_B o compósito de todos os corpos $k(a^{1/m})$ com $a \in B$, isto é K_B é o menor subcorpo de $\bar{k}$ contendo k e todos os corpos $k(a^{1/m})$, $a \in B$. K_B é unidamente determinado por B como um sub corpo de $\bar{k}$.

Sejam $a \in B$ e α uma raíz m-ésima de a. O polinômio $x^m - a$ fatora-se em fatores lineares em K_B, e daí K_B é Galosiana sobre k, pois todas as raízes de $x^m - a$ estão em K_B $\forall$ $a \in B$ e as raízes são distintas.

Sejam G o grupo de Galois de $K_B | k$ e $\sigma \in G$. Então $\phi(\alpha) = \omega_\sigma . \alpha$ para alguma m-ésima raíz da unidade $\omega_\sigma \in \mathbb{Z}_m \subset k^*$;

pois σ leva raíz em raíz.

Seja a aplicação $\phi: G \to Z_m$ definida por $\sigma \to \omega_\sigma$. Como podemos escrever $\omega_\sigma = \frac{\sigma(\alpha)}{\alpha}$, afirmamos que a aplicação ϕ é bem definida, pois α e α' são m-ésimas raízes de a, então $\alpha' = \xi\alpha$ para algum $\xi \in \mathbb{Z}_m^*$, daí

$$\frac{\sigma(\alpha')}{\alpha'} = \frac{\sigma(\xi\alpha)}{\xi\alpha} = \frac{\xi\,\sigma(\alpha)}{\xi\alpha} = \frac{\sigma(\alpha)}{\alpha}$$

, isto é a raiz da unidade ω_σ independe da escolha da m-ésima raíz de a. Obviamente ϕ é um homomorfismo de G em $\mathbb{Z}_m$.

Vamos denotar $\omega_\sigma = \frac{\sigma(\alpha)}{\alpha}$ por $\langle\sigma,a\rangle$. A aplicação

$\phi: G \times B \to Z_m$ dada por $(\sigma,a) \to \langle\sigma,a\rangle$ é bilinear. De fato, sejam a e b pertencentes a B e $\alpha^m = a$ e $\beta^m = b$ com $\sigma,\beta \in G$, então $(\alpha.\beta)^m = a.b$ e portanto

$$\frac{\sigma(\alpha\beta)}{\alpha\beta} = \frac{\sigma(\alpha)\sigma(\beta)}{\alpha.\beta} = \frac{\sigma(\alpha)}{\alpha} \cdot \frac{\sigma(\beta)}{\beta} = \langle\sigma,a\rangle.\langle\sigma,b\rangle$$

o que demonstra a linearidade da segunda variável. Dados σ e σ' pertencentes a G,

$$(\sigma\circ\sigma')(\alpha) = \sigma(\sigma'(\alpha)) = \sigma(\omega_{\sigma'}(\alpha)) = \omega_\sigma.\omega_{\sigma'} = \frac{\sigma(\alpha)}{\alpha} : \frac{\sigma'(\alpha)}{\alpha},$$

isto mostra a linearidade da primeira variável.

1.4.1. - Teorema

Sejam k um corpo, e $m > 0$ um inteiro primo com a ca -

racterística de k, e assumimos que a m-ésima raíz primitiva da unidade está em k.

Seja B um subgrupo de k contendo k^{*m} e seja $K_B = k(B^{1/m})$. Então, $K_B|k$ é Galosiana e abeliana de expoente m. Seja G seu grupo de Galois. A aplicação bilinear

$$\phi: G \times B \to Z_m \text{ dada por } (\sigma, a) \to \langle \sigma, a \rangle.$$

Então ϕ:

(1) Tem núcleo à esquerda 1 e à direita k^{*m}

(2) A extensão $K_B|k$ é finita se, somente se, $(B:k^{*m})$ e finito e neste caso temos

$$[K_B:k] = (B:k^{*m}).$$

Demonstração: Veja, Algebra, Serg Lang, Cap. VII, § 8. ∎

2 - TEOREMA DE RIEMANN-ROCH

2.1. - Preliminares

2.1.2. - Definição

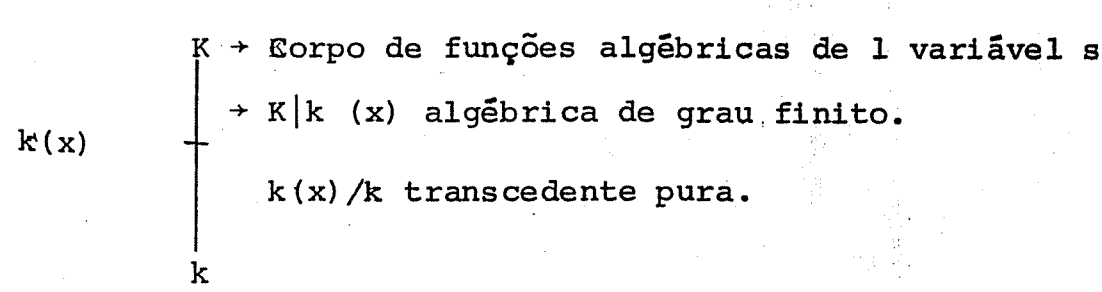
Sejam k um corpo e K uma extensão de k. Dizemos que K é um corpo de funções algébricas de uma variável sobre k se K é uma extensão de k do tipo finito e se o grau de transcedência de K sobre k é 1.

Seja K um corpo de funções algébricas de uma variável sobre k. Se x pertence a K e é transcedente sobre k, então K é uma extensão de grau finito de k(x). De fato, como o grau de transcedência de K sobre k é 1, o conjunto {x} é uma base de transcedência para K sobre k.

Seja y ε K-k. O conjunto {x,y} é algebricamente dependente sobre k, logo y é algébrico sobre k(x). Portanto K é algébrico sobre k(x). Sendo K uma extensão de tipo finito de k, então K é uma extensão de grau finito de k(x).

Assim, a extensão K de k se decompõe em duas extensões, uma transcedênte pura e a outra algébrica de grau finito.

O diagrama abaixo ilustra esta decomposição.



Assim, cada elementosde K-k pode assumir o papel da variável.

2.2. - Valorizações de um corpo de funções algébricas

Os três teoremas seguintes nos darão uma caracterização para as valorizações de um corpo K de funções algébricas de uma variável sobre k.

2.2.1. - Teorema

Seja K um corpo de funções algébricas de uma variável sobre k. Toda valorização não trivial v, de K sobre k é discreta.

Demonstração

Sejam v uma valorização de K sobre k, $x \in K$, transcedente sobre k, e $\omega = v_{|k(x)}$, a restrição de v para k(x) como uma valorização de k(x) sobre k é equivalentes as p(x)-ádicas ou a infinita, e portanto discreta, temos que ω é discreta. Logo v é também discreta (Veja proposição 1.2.12). ∎

2.2.2. - Teorema

Seja K um corpo de funções algébricas de uma variável sobre k. Para todo $x \in K^*$ tem-se:

(1) O número de valorizações discretas normalizadas v de $K|k$, tal que $v(x) \neq 0$ é finito.

(2) $v(x) = 0$, para toda valorização v de $K|k$, se, somente se, x

é algébrico sobre k.

Demonstração

(1) Consideremos $x \in K$ transcedente sobre k. Nas valorizações de k(x) sobre k, x só tem valor diferente de zero na x-ádica, v_o, e na infinita, v_∞, ou nas equivalentes. Como K é uma extensão algébrica de grau finito de k(x), então v_o e v_∞ tem um número finito de extensões à K. Daí as valorizações discretas normalizadas de K|k tais que $v(x) \neq 0$ são em número finito.

(2) De (1) temos que se $x \in K$ é transcedente sobre k, existe uma valorização v de K|k tal que $v(x) \neq 0$. Portanto se $v(x) \not> 0$ para toda valorização v de K|k, então x é algébrico sobre k.

Reciprocamente, sejam $x \in K^*$ algébrico sobre k, v uma valorização de K|k e $a_1, \ldots, a_n \in K$ nem todos nulos tais que $x^n + \ldots + a_{n-1}X + a_n = 0$.

Se $v(x) < 0$, temos, por um lado

$v(x^n + \ldots + a_n) = \infty$ e por outro lado

$v(x^n + \ldots + a_n) = nv(x) \neq \infty$ o que é um absurdo.

Se $v(x) > 0$, logo $v(x^n + \ldots + a_n) = v(a_n) = 0 \neq \infty$ que é um absurdo. Logo, se x é algébrico, então $v(x) = 0$ para toda valorização v de K|k.

■

2.2.3. - Teorema

Sejam K um corpo de funções algébricas de uma variá -

vel sobre k e v uma valorização de K sobre k. Então o grau n de v é finito.

Demonstração

Sejam v uma valorização de K|k, $x \in K$ transcendente sobre k e $\omega = v_{|k(x)}$.

Como K é uma extensão algébrica finita de k(x), pela desigualdade fundamental $[K_v:K_\omega] \leq [K:k(x)] < \infty$. Como $[K_\omega:k] < \infty$ segue-se que $[K_v:k]=[K_v:K_\omega].[K_\omega:h]$. Portanto temos provado o resultado. ∎

2.2.3.1. - Corolário

Se k é algebricamente fechado, então $K_v = k$ para toda valorização v de K|k e portanto toda valorização tem grau 1, neste caso.

2.3. - Divisores de K sobre k

Doravante vamos considerar K corpo de funções algébricas em um variável sobre k, com k algebricamente fechado em K.

Denotamos o grupo abeliano livre, gerado pelo conjunto das valorizações discretas normalizadas de K|k por Div(K|k).

Um elemento deste grupo será chamado de um Divisor de K|k.

Indexamos as valorizações discretas normalizadas de K|k por um conjunto de índices I, de modo que para cada $p \in I$.

v_p denota uma única valorização discreta normalizada de $K|k$. Um divisor X será denotado por:

$$X = \sum_{P\in I} n_p v_p, \text{ onde } n_p \text{ é um inteiro quase sempre nulo.}$$

(quase sempre nulo significa exceto para um número finito de índices).

Dado um divisor $X = \sum_{P\in I} n_p v_p$, chamamos de <u>grau de X</u>, o inteiro $d(X) = \sum_{P\in I} n_p d(v_p)$, onde $d(v_p)$ é o grau de v_p.

Claramente temos que $d(X) \in \mathbb{Z}$ e que $d(X\pm X') = d(X) \pm d(X')$ Ainda é claro que os divisores de grau zero formam um subgrupo de $Div(K|k)$. A título de exemplo, consideremos $K = k(x)$, x transcendente sobre k. Um divisor X de $K|k$ é da forma

$X = \sum_{\pi} n_\pi v_\pi + n_\infty v_\infty$ onde π percorre todos os polinômios mônicos irredutíveis em $k[x]$, e n_π quase sempre nulo. O grau de X é

$$d(X) = \sum_{\pi} n_\pi d(v_\pi) + n_\infty d(v_\infty) = \sum_{\pi} n_\pi \partial_\pi + n_\infty .$$

Para cada elemento $x \in K^*$, podemos formar o divisor $\sum_{P\in I} v_p(x) v_p$ (Isto tem sentido, pois as valorizações de $K|k$ tais que $v(x) \neq 0$ são em número finito), que é chamado de <u>Divisor Principal</u>, determinado por x e denotado por (x).

Como $v(xy) = v(x) + v(y)$ e $v(x^{-1}) = -v(x)$ para toda valorização v, temos $(xy) = (x) + (y)$ e $(x^{-1}) = -(x)$.

A aplicação $f: K^* \to Div(K|k)$ é

$$x \to (x)$$

um homomorfismo de grupos cuja imagem é o conjunto dos divisores

res principais e cujo núcleo é o conjunto dos elementos de K^* que são algébricos sobre k, que no caso por ser k algebricamente fechado em K, é k.

Dado $x \in K^*$, os divisores $(x)_o = \sum_{v_p(x)>0} v_p(x)\,v_p$ e $(x)_\infty = \sum_{v_p(x)<0} -v_p(x)\,v_p$ são chamados, respectivamente, de Divisor de zero de x e Divisor de polos de x.

Evidentemente $(x) = (x)_o - (x)_\infty$.

2.3.1. - Teorema

Sejam K um corpo de funções algébricas de uma variável sobre k e $x \in K$, transcendente sobre k. Então:

(1) $d((x)_o) = d((x)_\infty) = [K:k(x)]$

(2) $d((x)) = 0$, o grau de um divisor principal é zero.

Demonstração

A afirmação (2) é consequência de (1).

Para (1) basta mostrar que $d((x)_o) = [K:k(x)]$, pois

$$(1/x)_o = \sum_{v_p(1/x)>0} v_p(1/x)\,v_p = \sum_{v_p(x)<0} -v_p(x)\,v_p = (x)_\infty ,$$

isto é, os divisores de zero de 1/x são os divisores de polos de x e vice-versa e como $k(x) = k(1/x)$, se $d((x)_o) = [K:k(x)]$ então $d((x)_o) = [K:k(x)] = [K:k(1/x)] = d((1/x)_o) = d((x)_\infty)$.

Assim mostraremos que $d((x)_o) = [K:k(x)]$.

Sejam v uma valorização discreta normalizada de K|k

tal que $v(x) > 0$ e $\omega = v_{|k(x)}$

Como $\omega(x) > 0$, então ω é equivalente a valorização x-ádica não havendo mais que um número finito de valorizações discretas normalizadas, $v_1,\ldots,v_s$ de $K|k$ equivalentes aos prolongamentos $v_1', v_2',\ldots,v_s'$ de ω à K. Como v_i é equivalente a v_i', então $v_i = e_i v_i' \ \forall_i, i = 1,\ldots,s$, onde e_i é o índice de ramificação de v_i' sobre ω. Tomando $\omega(x) = 1$ então $v_i'(x)=1 \ \forall_i$, $i = 1,\ldots,s$ e daí $v_i(x) = e_i \underline{\forall} i$, $i = 1,\ldots,s$.

Sendo $d(v_i)=[K_{v_i}:k]=[K_{v_i}:k_\omega].[K_\omega:k] =[(K_{v_i}:k_\omega]=f_i$, índice de inércia de v_i sobre W, temos assim que $d((x)_o) = \sum_{i=1}^{s} v_i(x)d(v_i) = \sum_{i=1}^{s} e_i f_i$. Pela desigualdade fundamental, $d((x)_o) = \sum_{i=1}^{s} e_i f_i \leqslant [K:k(x)]$.

Vamos mostrar que a igualdade $d((x)_o) = [K:k(x)]$ se verifica.

Sejam A_ω o anel de valorização de ω e $S = k[x]-xk[x] \subset A_\omega$. É claro que $1 \in S$ e $S.S. \subset S$ (isto é, S é um sistema multiplicativo).

Consideremos A_ω' como sendo o fecho integral de A_ω em K e $k[x]'$ o fecho integral de $k[x]$ em K.

É fácil ver que $A_\omega = k[x]_S$. Como $k[x]$ é um domínio de integridade finito sobre o corpo k e K é uma extensão finita de k(x), então $k'[x]$ é um $k[x]$ - módulo finito, (veja [Z,S]$_1$, Capítulo V, § 4 , teorema 9), Assim $k[x]' = \sum_{i=1}^{m} k[x]\, u_i$, onde $\{u_1,u_2,\ldots,u_m\}$ é uma base finita de $k[x]'$.

Como $A_\omega' = [k[x]_S]' = (k[x]')_S = (\sum_{i=1}^{m} k[x]u_i)_S$

$$= \sum_{i=1}^{m} k[x]_S u_i = \sum_{i=1}^{m} A_\omega u_i$$

Portanto, A_ω' é um A_ω - módulo tipo finito. Pelos teoremas 19 e

20 do § 11 Cap. VI de $[Z,S]_2$ temos que

$$\sum_{i=1}^{s} e_i f_i = [K:k(x)] = d((x)_o)$$

Decorre da demonstração da proposição anterior, que se K é um corpo de funções algébricas de uma variável sobre k, vale a igualdade $[K:k(x)] = \sum_{i=1}^{m} e_i f_i$, chamada <u>igualdade fundamental</u>. ∎

2.3.2. - <u>Definição</u>

Dois divisores X e X' são ditos <u>Lineamento Equivalentes</u> se X-X' = (x) para algum $x \in K$, isto é, se X e X' diferem de um divisor principal.

Observemos que dois divisores linearmente equivalentes têm mesmo grau.

O grupo dos divisores de K é um grupo parcialmente ordenado, considerando a seguinte relação de ordem; $\sum_{P\in I} n_p v_p \geq \sum_{P\in I} n'_p v_p$ se, somente se, $n_p \geq n'_p$ $\forall P \in I$.

Em particular dizemos que um divisor $\sum_{P\in I} n_p v_p$ é positivo se $n_p \geq 0$ $\forall P \in I$.

Dado um divisor $X = \sum_{P\in I} n_p v_p$, consideremos o conjunto

$$L(X) = \{x \in K^*;\ (x) \geq -X\} \cup \{0\}$$

Assim, $x \in L(X) \iff \sum_{P \in I} v_p(x).v_p \geq -\sum n_p v_p \iff v_p(x) \geq -n_p \ \forall\ P \in I$.

2.3.3. - Lema $L(X)$ é um k-subespaço vetorial de K.

Demonstração

Sejam $x,x' \in L(X)$. Então $v_p(x) \geq -n_p$ e $v_p(x') \geq n_p$ $\forall\ P \in I$, e como $v_p(x+x') \geq \min\{v_p(x), v_p(x')\} \geq -n_p \ \forall\ P \in I$ temos $x+x' \in L(X)$.

Se $\lambda \in k$ e $x \in L(X)$, $v_p(\lambda x) = v_p(\lambda) + v_p(x) \geq -n_p$ $\forall\ P \in I$, portanto $\lambda x \in L(X)$.

Vamos denotar por $\ell(X)$ a dimensão de $L(X)$ sobre k. O nosso objetivo neste Capítulo é determinar $\ell(X)$.

2.3.4. - Proposição

(1) Sejam X e X' dois divisores tais que $X' \geq X$. Então $L(X') \supseteq L(X)$.

(2) Se $X = 0$, então $L(X) = k$

(3) Se $X < 0$, então $L(X) = \{0\}$

Demonstração

(1) Se $x \in L(X)$ então $(x) \geq -X \geq -X'$. Logo $x \in L(X')$ e $L(X) \subseteq L(X')$.

(2) É claro que se $X = 0$, $k \subset L(X)$.
Reciprocamente, se $x \in K-k$, x é transcendente sobre k e portanto, existe uma valorização v tal que $v(x) \neq 0$. Neste caso $x \notin L(0)$. Logo $L(0) \subset k$.

(3) Temos que $x \in L(x)$ se, somente se, $(x) > -X > 0$.
Se $x \in L(x)$, $x \neq 0$, então $d((x)) > 0$ que é um absurdo, pois $d((x)) = 0$. (Veja (2.3.1) (2)).
Logo $L(X) = \{0\}$.

■

2.3.5. - Lema

Se X e X' são linearmente equivalentes então $L(X)$ e $L(X')$ são k-isomorfos.

Demonstração

Basta provar no caso em que $X \neq X'$.
Seja $y \in k$ tal que $X-X' = (y)$. Observemos que se $x \in L(X)$, então, $(x) \geq -X$ e daí $(xy)=(x)+(y) \geq -X+(y) = X'$. Logo $xy \in L(X')$.
Se $x \in L(X')$ então $(x) \geq -X'$ é daí
$(xy^{-1}) = x-(y) \geq -X'-(y) = -X$, portanto $xy^{-1} \in L(X)$.
Consideremos agora os homomorfismo

$$h: L(X) \to L(X') \quad \text{e} \quad h^{-1}: L(X') \to L(X)$$
$$x \to xy \qquad\qquad x \to xy^{-1}$$

onde h e h^{-1} são recíprocos temos o k-isomorfismo entre $L(X)$ e $L(X')$.

■

2.3.6. - Lema

Sejam X um divisor de K|k e P ε I. Então, $L(X)$ é um subespaço de $L(X+v_p)$, e vale:

$$\dim_k \left(\frac{L(X+v_p)}{L(X)} \right) \leqslant d(v_p)$$

Se $L(X+v_p)$ tem dimensão finita sobre k, a desigualdade acima é equivalente a

$$\ell(X+v_p)-\ell(X) \leqslant d(v_p).$$

Demonstração

Como $X + v_p \geqslant X$, $L(X)$ é um k-subespaço de $L(X+v_p)$. O lema é evidente se $L(X+v_p) = L(X)$, pois $d(v_p) \geqslant 0$.

No outro caso, seja $x \in L(X+v_p)-L(X)$.

Façam os $X = \sum_{q \in I} n_q v_q$. Para todo $p \neq q$ temos

$$v_q(x) \geqslant -n_q \qquad e \qquad v_p(x) = -(n_p+1).$$

Se $y \in L(X+v_p)$, então $v_p(y) \geqslant -(n_p+1) = v_p(x)$ e $v_p(yx^{-1}) \geqslant 0$, que acarreta $yx^{-1} \in A_{v_p}$.

Sendo $\phi: L(X+v_p) \to K_{v_p}$

$$y \to yx^{-1} + M_{v_p}$$

Como v é trivial sobre k, a aplicação ϕ é k-linear.

Para que y pertença ao núcleo de ϕ é necessário e suficiente que $yx^{-1} \in M_{v_p}$. Isto é equivalente a $v_p(yx^{-1}) = v_p(y) - v_p(x) > 0$. Daí $v_p(y) > v_p(x) = -(n_p+1)$. Portanto $v_p(y) \geq -n_p$. Assim núcleo de ϕ é $L(X)$. Deste modo, podemos identificar $L(X+v_p)/L(X)$ como um subespaço vetorial de K_{v_p}, valendo

$$\dim_k (L(X+v_p)/L(X)) \leq [K_{v_p} : k] = d(v_p)$$

■

2.3.7. - Lema

Sejam X e X' divisores de K|k tais que $X' \geq X$. Então

$$\dim_k (L(X')/L(X)) \leq d(X')-d(X).$$

Em particular, se $\ell(X')$ é finito temos,

$$\ell(X')-d(X') \leq \ell(X)-d(X).$$

Demonstração

Seja $X'=X+v_1+v_2+\ldots+v_n$, com v_i valorizações não necessariamente distintas de K|k. Considerando a cadeia

$$X < (X+v_1) < (X+v_1+v_2) < \ldots < (X+v_1+\ldots+v_n) = X'$$

e denotando $X_i = x + v_1 + \ldots + v_i$, temos a sequência

$$L(X) \subset L(X_1) \subset \ldots \subset L(X_n) = L(X')$$

Da Álgebra Linear Clássica, segue-se que

$$\dim_k (L(X')/L(X)) = \dim_k (L(X_n)/L(X_{n-1})) + \ldots + \dim_k (L(X_1)/L(X))$$

Pelo lema 2.3.6 $\dim_k (\ell(X')/L(X)) \leq d(v_1) + \ldots + d(v_n) = d(X'-X) =$

$$= d(X') - d(X).$$

Se $L(X)$ e $L(X')$ são espaços vetoriais de dimensão finita sobre k, então

$\ell(X') - \ell(X) \leq d(X') - d(X)$. Ou, equivalentemente

$\ell(X') - d(X') \leq \ell(X) - d(X)$. ∎

2.3.7.1. - Corolário

Para todo divisor X, $\ell(X)$ é finita.

Demonstração

Dado um divisor X, existe um divisor Y tal que $Y \leq X$ e $Y < 0$. Por exemplo para $X = \sum_{p \in I} n_p v_p$ é suficiente tomar

$Y = \sum_{n_p<0} n_p v_p - v_o$ onde v_o é uma componente de X.

Como $L(X)/L(Y) = L(X)/\{0\}$ temos

$L(X)/L(Y) \simeq L(X)$. Pelo lema 2.3.7, $\ell(X) < d(X)-d(Y)$. Isto nos mostra que $\ell(X)$ é finito.

■

2.4. - Desigualdade de Riemann-Roch

2.4.1. - Teorema

Para todo divisor X de K|k $\ell(X)-d(X)$ tem uma cota inferior.

Demonstração

O lema anterior nos diz que a função $\ell(X)-d(X)$ é decrescente em X, sendo suficiente mostrar o teorema para $X \geq 0$ pois para $x < 0$ $\ell(X) = 0$ e $\ell(X)-d(X) = -d(X)$ tem o zero como cota inferior. se X não for nem > 0 e nem < 0 podemos substituir X por X' tal que $X' \geq 0$ e $X' \geq X$.e pelo lema 2.3.7 continua valendo a condição de decrescimento.

Vamos mostrar que para todo divisor $X \geq 0$ existe um divisor X' e um inteiro $n > 0$ tal que $X' \sim X$ e $X' \leq nY$.

Provaremos primeiramente, que para um $n > 0$, n suficientemente grande temos $\ell(nY) \geq nd(Y)-h$ onde h é uma constante que não depende de n.

Seja $Y = (y)_\infty$. Afirmamos que $\ell(nY) \geq n\,d(Y)-h$, para

n suficientemente grande e h uma constante que não depende de n.

Consideremos $d=d(Y) = [K:k(y)]$ e seja $\{z_1,z_2,\ldots,z_d\}$ uma base de K sobre k(y). Como K é uma extensão algébrica de k(y), os z_j são algébricos sobre k(y), multiplicando-os por elementos convenientes de k[y], podemos sem perda de generalidades, supor que os z_j são inteitos sobre k[y]. Para toda valorização v_p não figurando em Y temos $v_p(y) \geq 0$ e daí $y \in A_v$. Como $k \subset Av_p$, então $k[y] \subset Av_p$ e daí, $z_j \in Av_p$ (j=1,...,d), pois os z_j são inteiros sobre k[y].

Seja $-h_1 = \min_{i,j}\{v_{p_i}(z_j)\}$ onde v_{p_i} são valorizações que figuram em Y, isto é os prolongamentos normalizados a K da valorização v_∞ de k(y).

Consideremos os elementos $y^t z_j$ tais que $0 \leq t \leq n-h_1$ onde n é um inteiro conveniente. Portanto $v_{p_i}(y^t z_j) = t\, v_{p_i}(y) + v_{p_i}(z_j)$ e desde que $v_{p_i}(y) < 0$, temos

$$v_{p_i}(y^t z_j) \geq v_{p_i}(z_j) + (n-h_1)v_{p_i}(y) \geq -h_1 + (n-h_1)v_{p_i}(y)$$

$$\geq n v_{p_i}(y) - (1+v_{p_i}(y))h_1.$$

Como $1+v_{p_i}(y) \leq 0$ temos $v_{p_i}(y^t z_j) \geq n v_{p_i}(y)$. Por outro lado, $v_{p_i}(y^t z_j) \geq 0 \ \forall\ v_p \neq v_{p_i}$.

Dado que $nY = -\sum_{p \in I} n v_{p_i}(y)\, v_{p_i}$ temos $y^t z_j \in L(nY)$. Como os $y^t z_j$ são linearmente independentes sobre k, temos $\ell(nY) \geq d(nY-h_1)$. Logo $\ell(nY) \geq nd(Y)-h$ onde $h = dh_1$ é uma constante que não depende de n.

Supondo que $X = X_1+X_2$ onde X_1 e X_2 são dois divisores e que existem outros dois divisores X_1' e X_2' e dois inteiros

$n_1 \geq 0$ e $n_2' \geq 0$ tais $X_1' \sim X_2'$ e $X_1' \leq n_1 Y$ e $X_2' \leq n_2 Y$ e daí $X = X_1 + X_2 \sim X_1' + X_2' \leq (n_1 + n_2)Y$. Portanto é suficiente tomarmos $X' = X_1' + X_2'$. Assim temos que o nosso problema é aditivo.

Vamos agora determinar X' e o inteiro $n \geq 0$. Se $x = v_p$, dois casos temos a considerar. Ou temos $v_p \leq Y$ e aí não apresenta dificuldades, pois é suficiente tomarmos $x' = v_p$ e $n = 1$. Ou temos $v_p(y) \geq 0$, isto é, v_p não é componente de Y. Isto nos mostra que a restrinção ω de v_p a $k(y)$ não é a valorização infinita de $k(y)$. Como $M_{v_p} \cap k[y] = M_\omega$, então M_ω é um ideal principal, existindo um polinômio irredutível $F(y)$ em $k[y]$ tal que $M_\omega = \langle F(y) \rangle$. Como v_p é um zero de $F(y)$, então $(F(y)) \geq v_p$ e como os polos de $F(y)$ estão em Y, então existe um inteiro n tal que $(F(y)) \geq v_p - nY$. Tomemos então $X' = v_p \vee (F(y))$ e daí temos que $x' \sim v_p$ e $X' \leq nY$.

Seja $X' \leq nY$ e $X' \sim X$. Então

$$\ell(X) - d(X) = \ell(X') - d(X') \geq \ell(nY) - d(nY) > -h.$$

Assim $\ell(X) - d(X)$ tem uma cota inferios $\forall$ x $\in$ Div $(K|k)$. ∎

2.4.2. - Definição

O inteiro g, dado por $\inf_x(\ell(X) - d(X)) = -g+1$ é chamado gênero do corpo K de funções algébricas de uma variável sobre k.

Notemos que $\ell(X) - d(X) \geq -g+1$ e portanto g é o menor inteiro que satisfaz a desigualdade $\ell(X) \geq d(X) - g+1$; chamada Desigualdade de Riemann-Roch, e que se $X = 0$, então $\ell(X) = 1$ e

$d(X) = 0$. Logo $1 = 1-0 = \ell(0)-d(0) \geq -g+1$ e $g \geq 0$.

2.4.3. - Proposição

Existe um inteiro N tal que se $d(X) \geq N$, $\ell(X) = d(X)-g+1$.

Demonstração

Da desigualdade de Riemann-Roch existe um divisor Y tal que $\ell(Y)=d(Y)-g+1$. Seja $N = d(Y)+g-1$.

Seja X um divisor tal que $d(X) \geq N$. Pela desigualdade de Riemann-Roch

$$\ell(X-Y) \geq d(X-Y)-g+1 = d(X)-[d(Y)+g-1] = d(X)-N$$

Assim, existe $z \neq 0$ tal que $z \in L(X-y)$, isto é, $(z) \geq -X+Y$, $X \geq Y-(Z)$, seja $X' = Y-(Z)$. Como $d(X') = d(Y)$ e $\ell(X') = \ell(Y)$, (pois são equivalentes)

$$\ell(X') = d(X') - g+1$$

Como $X \geq X'$, pelo lema 2.3.7, $g = d(X')-\ell(X')+1 \leq d(X)-\ell(X)+1 \leq g$

Logo $\ell(X) = d(X)-g+1$.

∎

2.5. - Fórmula de Riemann-Roch

Dado um divisor X chamamos de índice de especialidade de X o inteiro $i(X) = \ell(X)-d(X)+g-1$. Da desigualdade de Riemann-Roch temos que $i(X) \geq 0$ para todo divisor X.

A função $\ell(X)-d(X)$ é decrescente pois se X e X' são dois divisores tais que $X' \geq X$ pelo lema 2.3.7 temos $\ell(X')-d(X') \leq \ell(X)-d(X)$. Assim a função $i(X)$ é decrescente e assume o valor zero para X suficientemente grande por exemplo se tomarmos X nas condições da proposição 2.4.2.

Dados dois divisores X e X' com $X' \geq X$, vamos dar uma interpretação para a diferença $i(X)-i(X')$. Para tanto vamos introduzir a noção de Adele.

Considerando I como o conjunto de índices que indexa as valorizações discretas normalizadas de $K|k$ damos a seguinte definição:

2.5.1. - Definição

Um adele é uma família $\alpha = (x_p)_{P\in I}$ de $K^I = \prod_{P\in I} K^P$ com (x_p) pertencente a K e $v_p(x_p) \geq 0$, exceto para um número finito de índices p.

Denotamos por $\mathcal{A}$ o conjunto dos adeles. É claro ver que $\mathcal{A}$ é um subanel de K^I.

Dado um adele $\alpha = (x_p)_{P\in I}$ escrevemos $v_p(\alpha)$ ao invés de $v_p(x_p)$. Consideremos a aplicação que associa um elemento x de K ao elemento $(x_p)_{P\in I}$ onde $x_p = x$ para todo $P \in I$. Assim $(x_p) = (x,..,x,..,)$. Como $v_p(x) \neq 0$ para um número fimito de p pertencentes a I e $v_p(x) = 0$, para toda valorização v_p de $K|k$ se, somente se, x é algébrico sobre k, temos que $(x_p)_{P\in I}$ pertence a $\mathcal{A}$. A aplicação definida de K em $\mathcal{A}$ é um homomorfismo injetivo de anéis. Tais adeles são chamados de Principais e formam um sub-anel de $\mathcal{A}$, o qual identificamos com K. Dizemos ainda, que K esta diagonalmente imerso em $\mathcal{A}$.

Para qualquer divisor $X = \sum_{P \in I} n_p v_p$, consideremos o conjunto

$$\mathcal{A}(x) = \{\alpha \in \mathcal{A} : v_p(\alpha) \geq -n_p \ \forall p \in I\}.$$

Observemos que $\mathcal{A}(x)$ é um espaço vetorial sobre k e que $L(x) = \mathcal{A}(x) \cap K$. Além do mais, se $X' \geq X$, então $\mathcal{A}(X') \supset \mathcal{A}(X)$.

2.5.2. - Lema

Tem-se $\dim_k \left(\frac{\mathcal{A}(x+v_p)}{\mathcal{A}(x)} \right) = d(v_p)$ e, mais geralmente se X, X' são dois divisores tais que $X' \geq X$, então

$$\dim_k \left(\frac{\mathcal{A}(X')}{\mathcal{A}(x)} \right) = d(X') - d(X).$$

Demonstração

Vamos supor, inicialmente, que $X' = X + v_p$, para alguma valorização v_p.

Seja $X = \sum_R n_R v_R$. Então

$$\mathcal{A}(x) = \{\alpha \in \mathcal{A} ; v_R(\alpha) \geq -n_R \ \forall R \in I\}.$$

Seja $a \in K$ tal que $v_p(a) = -(n_p+1)$

Consideremos a aplicação k-linear

$$\psi: \mathcal{A}(x+v_p) \to K_{v_p}$$
$$(x_R) \to a^{-1} x_p + M_{v_p}.$$

(i) ψ é bem definida, pois,

$$v_p(a^{-1}x_p) = v_p(a^{-1}) + v_p(x_p) = -v_p(a) + v_p(x_p) \geq n_p + 1 + v_p(x_p) \geq 0,$$

isto é $a^{-1}x_p \in A_{v_p}$.

(ii) ψ é um homomorfismo de k-espaços vetoriais.

(iii) o núcleo de ψ é $\mathcal{A}(X)$, pois $\psi(y_p) = 0$ se, e somente, se $a^{-1}y_p \in M_{v_p}$, isto é, $v_p(a^{-1}y_p) \geq 1$.
Mas $v_p(a^{-1}y_p) = v_p(a^{-1}) + v_p(y_p)$ e portanto $\psi(y_p) = 0$ se, somente se $v_p(y_p) \geq -v_p(a^{-1}) = 1-(n_p+1) = -n_p$, isto é, se, somente se $(y_p) \in \mathcal{A}(X)$.

(iv) ψ é sobrejetivo, pois se $\overline{z} \in K_{v_p}$, consideremos o adele $(x_p)_{R \in I}$ tal que $x_R = 0 \ \forall \ R \neq P$ e $x_p = az$. Temos assim que (x_R) é um adele em $\mathcal{A}(X+v_p)$ e daí ψ é sobrejetiva.

Pelo Teorema Fundamental dos Homomorfismo $\mathcal{A}(X+v_p)/\mathcal{A}(X)$ é k-isomorfo a K_{v_p}, e portanto

$$\dim_k \left(\frac{\mathcal{A}(X+v_p)}{\mathcal{A}(X)} \right) = d(v_p)$$

mostramos assim a primeira afirmação.

Para o caso geral consideremos agora,
$X' = X+v_1+v_2+\ldots+v_n$, v_i valorizações de $K|k$, e

a cadeia

$$X < X + v_1 < X + v_1 + v_2 < \ldots < X + v_1 + \ldots + v_n = X'$$

obtemos assim a sequência

$$\mathcal{L}(X) \subseteq \mathcal{L}(x+v_1) \subseteq \ldots \subseteq \mathcal{L}(X+v_1+v_2+\ldots+v_n) = \mathcal{L}(X')$$

Da Álgebra Linear Clássica, temos

$$\dim_k (\mathcal{L}(X')/(\mathcal{L}(X)) = \dim_k (\mathcal{L}(X_n)/(\mathcal{L}(X_{n-1}) + \dim_k (\mathcal{L}(X_{n-1})/(\mathcal{L}(X_{n-2}) +$$

$$+\ldots+ \dim_k (\mathcal{L}(X_1)/(\mathcal{L}(x)).$$

Como já provamos na redução que

$$\dim_k (\mathcal{L}(X_{i+1})/\mathcal{L}(X_i)) = d(v_i) \quad \forall i,\ i = 1,\ldots,n, \text{ temos}$$

$$\dim_k (\mathcal{L}(X')/\mathcal{L}(X) = d(v_n)+d(v_{n-1})+\ldots+\dim(v_1) = d(v_n+v_{n-1}+\ldots+v_1) =$$

$$d(X'-X) = d(X')-d(X).$$

∎

2.5.3. - Lema

Sejam X e X' dois divisores tais que $X' \geq X$. Então

$$\dim_k ((\mathcal{L}(X')+K)/(\mathcal{L}(X)+K)) = i(X)-i(X')$$

Demonstração

Como $X' \geq X$, $\mathcal{A}(X) \subset \mathcal{A}(X')$, e

$$\mathcal{A}(X')+K = \mathcal{A}(X')+(\mathcal{A}(X)+K)$$

Seja $E = (\mathcal{A}(X')+K)/(\mathcal{A}(X)+K)$.

Pela primeira lei dos módulos (Veja $[P;S]_2$).

$$E = (\mathcal{A}(X')+(\mathcal{A}(X)+K))/(\mathcal{A}(X)+K) \cong \mathcal{A}(X')/\mathcal{A}(X') \cap (\mathcal{A}(X)+K).$$

Como $(\mathcal{A}(X') \cap (\mathcal{A}(X)+K)) = \mathcal{A}(X)+\mathcal{A}(X') \cap K = \mathcal{A}(X) + L(X')$

temps $E \cong \mathcal{A}(X')/(\mathcal{A}(X)+L(X'))$. Pela segunda lei dos módulos

$$E \cong (\mathcal{A}(X')/\mathcal{A}(X))/((\mathcal{A}(X) + L(X'))/\mathcal{A}(X)$$

Novamente pela primeira lei dosmódulos temos

$$E = (\mathcal{A}(X')/(\mathcal{A}(X))/(L(X')/(\mathcal{A}(X) \cap L(X'))$$

$E = (\mathcal{A}(X')/\mathcal{A}(X))/(L(X')/L(X))$, pois

$$L(X') \cap \mathcal{A}(X) = (\mathcal{A}(X') \cap K) \cap \mathcal{A}(X) = \mathcal{A}(X) \cap K = L(X).$$

Podemos então escrever,

$$\dim_k E = \dim_k(\mathcal{A}(X')/\mathcal{A}(X)) - \dim_k(L(X')/L(X))$$

$$\dim_k E = [d(X') - d(X)] - [\ell(X') - \ell(X)]$$

$$\dim_k E = [\ell(X) - d(X)] - [\ell(X') - d(X')]$$

$$\dim_k E = [i(X) - g + 1] - [i(X') - g + 1] = i(X) - i(X').$$

■

2.5.4. - Lema

Seja X um divisor qualquer. Então

$$\dim_k(\mathcal{A}/(\mathcal{A}(X)+K)) = i(X)$$

Demonstração

Mostraremos primeiramente que o conjunto dos adeles $\mathcal{A} = U_{X' \geq X} \mathcal{A}(X')$ e em consequência $\mathcal{A} = \underset{X' \geq X}{U}(\mathcal{A}(X')+K)$ uma vez que $\mathcal{A}(X') \subset \mathcal{A}(X)+K$, e ainda $(\mathcal{A}/(\mathcal{A}(X)+K)) = (U_{X' \geq X}(\mathcal{A}(X') + K)/(\mathcal{A}(X)+K)$.

Sejam $\alpha = (x_p)_{p \in I} \in \mathcal{A}$, $X = \sum_{p \in I} n_p v_p$, e $n'_p = \max\{n_p, -\min(0, -v_p(\alpha))\}$. Temos o divisor $X' = \sum_{p \in I} n'_p v_p$ satisfaz $X' \geq X$. Como $v_p(\alpha) \geq -n_p \ \forall\ p \in I$ temos que $\alpha \in \mathcal{A}(X')$, e e $\mathcal{A} \subset U_{X' \geq X}(X')$.

Como $\mathcal{A} \supset U_{X' \geq X}(X')$ concluimos que $\mathcal{A} = U_{X' \geq X}(X')$.

Se X_1 e X_2 são dois divisores tais que $X_1 \geq X$ e $X_2 \geq X$ existe um divisor X_3 tal que $X_3 \geq X_1$ e $X_3 \geq X_2$. Assim, sem perdas de generalidades, podemos dizer que $\mathcal{A} = U_{X' \geq X}(\mathcal{A}(X') + K)$ tal que $\mathcal{A}(X') \supset \mathcal{A}(X)$ para $X' \geq X$.

Para X' suficiente grande temos $i(X') = 0$ e portanto para tal X', pelo Lema 2.5.3., temos

$$\dim_k((\mathcal{A}(X') + K)/(\mathcal{A}(X) + K)) \leq i(X).$$

Seja X'' um divisor tal que $X'' \geq X'$, onde X' é como acima.

Assim, $\dim_k((\mathcal{A}(X'') + K)/(\mathcal{A}(X') + K)) = i(X') - i(X'') = 0$, daí

$$\mathcal{A}(X'') + K = \mathcal{A}(X') + K$$

Como cada elementosde $\mathcal{A}$ está contido em algum espaço $\mathcal{A}(X'')$ para X'' suficientemente grande, $X'' \geq X'$ concluimos que $\mathcal{A}(X'') + K = \mathcal{A}$. Provamos então, que

$$\max\{\dim_k((\mathcal{A}(X') + K)/(\mathcal{A}(X) + K))\} = i(X).$$

Isto mostra que $\mathcal{A} \supset \mathcal{A}(x) + K$ é a reunião de espaços vetoriais de dimensão menor ou igual a $i(X)$, e sendo a maior dimensão assumida.

Logo $\dim_k(\mathcal{A} \supset (\mathcal{A}(X) + K)) = i(x)$ ∎

Vamos considerar formas k-lineares sobre $\mathcal{A}$ que são nulas sobre os sub-espaços vetoriais da forma $\mathcal{A}(X) + K$, para um divisor X conveniente. Uma tal forma é chamada de uma Diferencial de Weil ou Duadele.

Dado um divisor X, denotamos por $\Omega(x)$ o espaço vetorial sobre k, dos duadeles nulos sobre $\mathcal{A}(x) + K$, isto é:

$$\Omega(X) = \left\{ \begin{array}{l} \omega: \mathcal{A} \to k;\ \omega(\mathcal{A}(X)+K) = 0 \\ \\ \omega \text{ k-linear} \end{array} \right\}$$

Como $\Omega(X)$ é o dual do espaço vetorial $\mathcal{A}/\mathcal{A}(X)+K$ sobre K, que é de dimensão finita, temos que $\dim_k(\Omega(X)) = i(X)$.

Um duadele ω anulando-se em $\mathcal{A}(X')$ e $\mathcal{A}(X")$ anula-se também em $\mathcal{A}(X') + \mathcal{A}(X")$, pois ω é uma forma k-linear.

2.5.5. - Definição

Sejam $X' = \sum_{P\in I} n'_p v_p$ e $X" = \sum_{P\in I} n"_p v_p$ divisores. Definimos $\sup\{X', X"\}$ como sendo o divisor cujas coordenadas são dadas por $\max\{n'_p, n"_p\}$.

2.5.6. Proposição

$$\mathcal{A}(X') + \mathcal{A}(X") = \mathcal{A}(\sup(X', X")).$$

Demonstração

Trivialmente $\mathcal{A}(X') + \mathcal{A}(X") \subset \mathcal{A}(\sup(X', X"))$.

Consideremos agora $\alpha = (x_p)_{P\in I} \in \mathcal{A}(\sup(X', X"))$.

Se $X' = \sum_{P\in I} n'_p v_p$ e $X" = \sum_{P\in I} n"_p v_p$ então $v_p(\alpha) \geq -\sup\{n'_p, n"_p\}$.

Sejam $I' = \{P \in I;\ n'_p \geq n''_p\}$ e $I'' = \{P \in I;\ n'_p < n''_p\}$.
Em I' o máx$\{n'_p, n''_p\}$ é n'_p e em I'' é n''_p.
Consideremos os adeles $\alpha' = (x'_p)$ e $\alpha'' = (x''_p)$ tal que
$x'_p = x_p \ \forall\ P \in I'$ e $x'_p = 0 \ \forall\ P \in I''$ e $x''_p = 0 \ \forall P \in I'$ e
$x''_p = x_p \ \forall\ P \in I''$. Temos assim $\alpha' \in \mathcal{A}(X')$ e $\alpha'' \in \mathcal{A}(X'')$ e
$\alpha = \alpha' + \alpha'' \in \mathcal{A}(X') + \mathcal{A}(X'')$.

■

2.5.7. - Proposição

Dado um duadele ω, não nulo, existe um maior divisor X tal que $\omega(\mathcal{A}(X)+K) = 0$.

Demonstração

Afirmamos que existe um inteiro N, tal que para cada divisor Y tal que $d(Y) > N$, então $\Omega(Y) = \{0\}$.

De fato, pela desigualdade de Riemann-Roch, sabemos que se Y é um divisor qualquer, então $i(Y) = \ell(Y) - d(Y) + g - 1 > 0$ e que existe um inteiro N tal que se Y é um divisor com $d(Y) > N$, então $i(Y) = \ell(Y) - d(Y) + g - 1 = 0$.
Pelo lema 2.5.4. temos que para cada divisor X,

$$i(X) = \dim_k (\mathcal{A}/\mathcal{A}(x)+K),$$

Assim, se $d(Y) > N$ temos

$0 = i(Y) = \dim_k (\mathcal{A}/\mathcal{A}(Y)+K)$. Logo $\mathcal{A} = \mathcal{A}(X)+K$,
portanto $\Omega(Y) = \{0\}$.

Agora, veja ω um duadele não nulo. Por definição, existe um divisor X tal que $\omega \in \Omega(X)$, isto é $\omega(\mathcal{A}(X)+K) = 0$. Pela afirmação anterior, temos que $d(X) < N$. Logo podemos esco -

lher um divisor X' tal que:

(i) $\omega(\mathcal{A}(X') + K) = 0$

(ii) $d(X')$ é o maior possível (já que $d(X') < N$).

Afirmamos agora que um X' obtido acima tem a propriedade desejada. De fato, seja X" um outro divisor tal que $\omega(\mathcal{A}(X")+K) = 0$. Então $\omega((\mathcal{A}(X')+\mathcal{A}(X"))+K) =$ $\omega(\mathcal{A}(\sup(X',X")+K) = 0$.

Naturalmente, sup(X',X") é um divisor, e temos $\sup(X',X") \geq X'$ logo $d(\sup(X',X") \geq d(X')$. Mas então, $d(\sup(X',X")) = d(X)$, pela maximalidade de d(X'). Temos assim $\sup(X',X") \geq x'$ e $d(\sup(X',X") = d(X')$. Então $\sup(X',X") = X'$ e portanto $X' \geq X"$,

Assim, para qualquer outro divisor X",tal que $\omega(\mathcal{A}(X")+K) = 0$, temos $X' \geq X"$. Isto é, X' é o maior divisor.

∎

2.5.8. - Definição

Seja ω um duadele não nulo. Chamamos divisor de ω ao maior divisor X tal que $\omega(\mathcal{A}(X)+K) = 0$.

Denotamos o divisor de ω por (ω) que chamamos de divisor canônico de ω. Assim, podemos definir Ω(X) como sendo:

$$\Omega(X) = \{\omega;\ (\omega) > X\}$$

2.5.9. - Proposição - Existe duadele não nulo.

Demonstração

Seja $X \in Div(K|k)$ tal que $X < 0$ e $d(X) < -1$ por exemplo, $X = \sum_{n_p < 0} (n_p v_p) - v_o$, onde v_o é uma valorização tal que $d(v_o) = 1$. Como $\ell(X) = 0$, a fórmula $\ell(X) = d(X) - g + 1 + i(X)$ nos dá $i(X) = g - (d(X)+1)$ e como $g \geq 0$ e $(d(X)+1) \leq 0$, então $i(X) \geq 0$. Como $\dim_k(\Omega(X)) = i(X)$ $\forall$ $x \in Div(k|k)$ temos que existe duadele não nulo.

■

Seja ω um duadele e $x \in K$, $x \neq 0$. Definimos $x\omega$ como sendo o duadele tal que $(x\omega)\alpha = \omega(x\omega)$ $\forall$ $\alpha \in$. Temos assim que $x\omega$ é uma aplicação k-linear, que $(x\omega)(K) = 0$, pois se $\alpha \in K$ então $x.\alpha \in K$ logo $0 = \omega(\alpha x) = (x\omega)(\alpha)$. Além do mais $\omega(\mathcal{A}(x)) = 0$ se, somente se, $x\omega(\mathcal{A}(X+(x)) = 0$. De fato, sejam $X = \sum_{p \in I} n_p v_p$ e $\alpha = (x_p) \in \mathcal{A}$, $X + (x) = \sum [n_p + v_p(x)] v_p$. Temos: $\alpha \in \mathcal{A}(X+(x)) \Leftrightarrow v_p(x_p) \geq -[n_p + v_p(x)] \Leftrightarrow v_p(x.x_p) \geq -n_p$ $x\alpha \in \mathcal{A}(X)$. Agora $\omega(\mathcal{A}(X)) = 0$ então $\forall$ $\alpha \in \mathcal{A}(X+(x))$, $x\omega(\alpha) = \omega(x\alpha) = 0$, isto é $x\omega(\mathcal{A}(x+(x))) = 0$.

Reciprocamente, se $x\omega(\mathcal{A}(X+(x)) = 0$, então, para cada $\alpha \in \mathcal{A}(x)$, $\alpha = x(x^{-1}.\alpha)$, $x \neq 0$, $x^{-1}.\alpha \in \mathcal{A}(X+(x))$. Portanto, $x\omega(x^{-1}\alpha) = 0 \Leftrightarrow \omega(\alpha) = 0$.

Assim temos que $(x\omega) = (x) + (\omega)$.

■

2.5.8. - Teorema Os duadeles formam um espaço vetorial de dimensão 1 sobre K, isto é:

$$\dim_k \Omega(x) = 1$$

emonstração

Pelo corolário (2.5.8.1), sabemos que $\Omega(X) \neq \{0\}$.

Suponhamos por absurdo que existem dois duadeles que ejam linearmente independentes sobre K, digamos $\omega' \in \Omega(X')$ e $\omega'' \in \Omega(X'')$. Seja X um divisor tal que $X \leqslant X'$ e $X \leqslant X''$. Então $\Omega(X) \supseteq \Omega(X')$ e $\Omega(X) \supseteq \Omega(X'')$. Assim, ω' e ω'' pertencem a $\Omega(X)$.

Seja Y um divisor arbitrário e seja $\{z_1, z_2, \ldots, z_m\}$ ma k-base de $L(Y)$. Então $z_i\omega'$, $z_i\omega'' \in \Omega(X-(z_i)) \subseteq \Omega(X-y)$, $i = 1, \ldots, m$, pois $(z_i) > -Y \ \forall_i$.

Como ω' e ω'' são linearmente independentes sobre K, como $z_1, z_2, \ldots, z_m$ são linearmente independentes sobre k, concluimos que $z,\omega', \ldots, z_m\omega$ e $z_1\omega'', \ldots, z_m\omega''$ são linearmente independentes sobre k. Em particular $2m \leqslant i(X-Y)$.

Aplicando aos divisores Y e X-Y a equação $(X) = \ell(X) + d(X) - g + 1$ obtemos:

$[d(Y)+1-g-i(Y)] < \ell(X-Y) - d(X-Y) - 1 + g$, isto é,

$(Y) \leqslant \ell(X-Y) - d(X) - 3 + 3g - 2i(Y)$ para cada divisor Y.

Escolhamos Y tal que $[d(Y)] = n$, n suficientemente rande. Então $i(Y) = 0$ e $d(X-Y) < 0$. Logo $\ell(X-Y) = 0$.

Portanto $d(Y) \leqslant -d(X) - 3 + 3g$, contradição pois, $d(Y)] = n$, n suficientemente grande.

Provamos, assim que $\dim_K \Omega(X) = 1$

∎

2.5.9.1. - Carolário

Os divisores dos duadeles não nulos em $\Omega(X)$, X fixo, são todos linearmente equivalentes.

Demonstração

Sejam ω e ω' dois duadeles, não nulos. Então existe $x \in K$ tal que $\omega' = x\omega$. Logo $(\omega') = (x)+(\omega)$ o que mostra serem (ω) e (ω') equivalentes. ∎

2.6. - Teorema Geral de Riemann-Roch

2.6.1. - Teorema

Seja C um divisor canônico de um duadele. Para todo divisor X, temos

$$i(x) = \ell(C-X) \quad \text{e} \quad \ell(X) = d(X)-g+1 + \ell(C-X)$$

Demonstração

Sejam $\omega \in \Omega(X)$ tal que $C=(\omega)$ e $x \in K$.

Temos $(x\omega) \geq X \Leftrightarrow (x) + (\omega) \geq X \Leftrightarrow (x) \geq X-(\omega) \Leftrightarrow x \in L(-X+(\omega))$. Como $L(C-X)$ é um espaço vetorial sobre k de dimensão $L\ell(C-X)$ e como os duadeles $x\omega$ tal que $(x\omega) \geq X$ forma um subespaço de $\Omega(X)$, de dimensão $i(X)$, temos então

$i(X) = \ell(C-X)$, daí $\ell(X) = d(X)+g+1+\ell(C-X)$ ∎

Como $K_{v_\infty} = k$, então $d(v_i) = [K_{v_i}:k] = f_i$. Seja X o divisor dado por $X = \sum_i e_i v_i$. Então

$$d(X) = \sum_i e_i d(v_i) = \Sigma e_i f_i = [K:k(x)] = \partial f = 2.$$

Assim, X pode ter as seguintes fprmas:

(i) $X = v_1 + v_2$, com $e_i = e_2 = f_1 = f_2$, chamada de forma decomposta.

(ii) $X = v_i$, com $e_1 = 1$ e $f_1 = 2$, chamada de forma Inerte.

(iii) $X = 2v_i$, com $e_1 = 2$ e $f_1 = 1$, chamada de forma ramificada.

Observemos que $z \in L(nX)$ se, somente se, $(z) \geq -nX$ se, somente se, $v_i(z) \geq -ne_i \ \forall_i$, $v(z) \geq 0$ para $v \neq v_\infty$.

2.6.2. - Lema

Sejam k um corpo de característica $\neq 2$ e $K = k(x,y)$ um corpo de funções algébricas de uma variável sobre k, com $y^2 = f(x)$, onde f(x) é um polinômio livre de quadrados em $k[x]$. Sejam v_i os prolongamentos da valorização infinita de k(x) e e_i seus respectivos índices de ramificação e $X = \sum_i e_i v_i$ um divisor de $K|k$. Se $z \in L(nX)$, então $z = a(x) + yb(x)$ com a a(x) e b(x) pertencentes a $k[x]$.

Demonstração

Sendo $y^2 = f(x)$ então os elementos de K são da forma $z = a(x) + yb(x)$ com a(x) e b(x) pertencentes a k(x).

Consideremos o automorfismo σ de $K|k(x)$ definido por

2.6.1.1. - Corolário

(1) $\ell(C) = g$

(2) $d(C) = 2g-2$

(3) Se X é um divisor tal que $d(X) \geq 2g-2$

então $\ell(x) = d(x)-g+1$

Demonstração

(1) Sendo $X = 0$, então $i(0) = \ell(C) = 1+g-1 = g$

(2) Sendo $X = C$, então $\ell(C) = d(C)-g+1+1$ logo

$d(C) = g+g = 2$ e daí $d(C) = 2g-2$.

(3) Se $d(X) > 2g-2$, então $d(C-X) = d(C)-d(X) \leq 2g-2-2g+2 = 0$.

Assim $d(C-X) < 0$, para $d(X) > 2g-2$.

Como para todo $x \in K^*$, $d((x)) = 0$, temos $L(C-X) \neq \{0\}$, pois se $0 \neq x \in L(C-X)$ então $(x) \geq X-C$ e como $0 = d((x)) \geq d(X-c) > 0$ temos um absurdo. Logo $L(C-X) = \{0\}$ e daí $L(C-X) = 0$ pelo Teorema Geral de Riemann-Roch $\ell(X) = d(x) -g+1$. ∎

Como aplicação prática do teorema de Riemann-Roch vamos determinar um algorítmo para encontrar o gênero de um corpo de funções algébricas de uma variável sobre k, $K|k$, no caso em que a característica de k é diferente de 2 e $K = k(x,y)$ com $y^2=f(x)$, $f(x) \in k[x]$ um polinômio sem fatores múltiplos. Para tanto vamos fazer algumas considerações sobre os prolongamentos da valorização infinito, v_∞, e sobre um divisor bem particular de $K|k$.

Sejam v_∞ a valorização de k(x) e v_i os seus prolongamentos à K, k algebricamente fechado em K, e e_i e f_i seus índices de Ramificação e Inércia, respectivamente.

$\sigma(a(x)+yb(x) \triangleq a(x)-yb(x)$.

Se $v \neq v_\infty$ então $(v\circ\sigma)(a(x)+yb(x))=v(a(x)-yb(x)) \geq 0$.

Logo $\omega(a(x)-yb(x)) \geq 0$ para cada valorização ω de $K|k$ que não prolonga v_∞. Como $[a(x)+yb(x)]+[a(x)-yb(x)]$ e $[a(x)+yb(x)]$ $[a(x)-yb(x)]$ têm valores positivos para toda valorização de $k(x)$. Concluimos que $[a(x)+yb(x)]+[a(x)-yb(x)]$ e $[a(x)+yb(x)].[a(x)-yb(x)]$ pertencem a $k[x]$ e como a característica de k é $\neq 2$ temos que $a(x) \in k[x]$ e como f é livre de quadrados em $k[x]$ temos que $f(x)b^2(x) \in k[x]$ e portanto $b(x) \in k[x]$. ∎

Sob as hipóteses do lema 2.6.2 vamos agora determinar $\ell(nX)$ para n suficientemente grande. Para tanto, vamos considerar em separado o caso em que o grau de f é par do caso em que o grau de f é ímpar.

Caso 1 - O grau de f é ímpar

Como $v_\infty(x) = -1$, então $v_i(x) \triangleq -e_i$ e $v_i(f(x))=-e_i\partial f$. Sendo $y^2=f(x)$, então $2v_i(y) = -e_i(2m+1)$, como $v_i(y) \in \mathbb{Z}$ então, e_i é par. Temos então o caso em que X é ramificado, portanto existe uma única valorização, v_1 com $e_1=2$ e $f_1 = 1$, daí $X=2v_1$. Assim $z \in L(nX)$ se, somente se, $v_1(z) \geq -2n$ e $\omega(z) \geq 0$ $\forall$ $\omega \neq v_1$. Como $v_1(a(x) = -2\partial(a(x))$ e $v_1(yb(x)) = v_1(y)+v_1(b(x)= -(2m+1) - 2\partial(b(x))$, então $v_1(a(x)) \neq v_1(yb(x))$ e portanto $v_1(z) = \min\{-2\partial(a(x)),-2\partial b(x)-(2m+1)\}$. Portanto, $v_1(z) \geq -2n$, se, somente se, $\partial(a(x) \leq n$ e $\partial(b(x)) \leq n-m-1/2$. Mostramos assim que $\ell(nX) = (n+1)+(n-m-1+1) = 2n-m+1$.

Caso 2 - O Grau de f é par, digamos $\partial f = 2m$

Como $v_i(x) = -1$, $v_i(y) = \frac{1}{2} v_i(f) = -\frac{1}{2} \partial f = -m$. Logo $v_i(y/x^m) = 0$. Sendo f de grau par, podemos escrevê-lo como sendo:

$f(x) = a_o x^{2m} + a_1 x^{2m-1} + \ldots + a_{2m}$, $a_j \in k$, $a_o \neq 0$

$j = 0,1,\ldots,2m$.

Temos $(y/x^m)^2 = a_o + (a_1/x) + \ldots + (a_{2m}/x^{2m})$.

Seja A_{v_i} o anel de valorização de v_i e M_{v_i} seu ideal maximal.

Consideremos o homomorfismo canônico

$$h_i : A_{v_i} \to \frac{A_{v_i}}{M_{v_i}}$$

$$x \to x + M_{v_i}$$

sendo $v_\infty(x) < 0$, então $v_\infty(1/x) > 0$. Então $v_i(1/x) > 0$.

Logo $h_i(1/x) = 0$ e portanto $h_i((y/x^m)^2) = h_i(a_o) = a_o$.

Se $a_o \notin k^2$, então $h_i(y/x^m) \notin k$, portanto $k \subsetneq K_{v_i}$, isto mostra que $1 < [K_{v_i} : k] \leq 2$. Logo, $f_i = 2$. Temos assim o caso em que X é Inerte, isto é, $X = v_i$ com $e_1 = 1$ e $f_1 = 2$.

Seja $z = a(x) + yb(x)$, com

$a(x) = c_o x^s + \ldots + c_s$, com $c_j \in k$, $c_o \neq 0$

$b(x) = c'_o x^{s'} + \ldots + c_{s'}$, com $c'_j \in k$, $c'_o \neq 0$

satisfazendo a equação, $\partial a(x) = \partial b(x) + \frac{\partial f(x)}{2}$, isto é, $s = s' + m$.

Notemos que $v_1(a(x)) = -s$ e $v_1(yb(x)) = -(s'+m)$. Uma nova expressão para z é:

$$Z = (c_o + c'_o \frac{y}{x^m}) x^s + (c_1 + c'_1 \frac{y}{x^m}) x^{s-1} + \ldots + (c_s + c'_s \frac{y}{x^m})$$

com a hipótese de $s = s'+m$. Para $v_1(z) > \min\{v_1(a(x)), v_1(yb(x))\}$ precisamos que $v_1(c_o+c'_o \frac{y}{x^m}) > 0$, isto é equivalente a $h_1(c_o+c'_o\, y/x^m) = 0$. Como $h_1(y/x^m) = -(\frac{c_o}{c'_o}) \varepsilon k$, temos $a_o = h_1(\frac{y}{x^m})^2 = (\frac{c_o}{c'_o})^2$, portanto $a_o \varepsilon k^2$ o que contraria a escolha do a_o. Portanto, devemos ter $v_1(c_o+c'_o \frac{y}{x^m}) = 0$ e consequentemente $v_1(z) = \min\{v_1(a(x), v_1(yb(x))\}$.

A condição $v_1(z) \geq -n$ é equivalente a $\partial(a(x)) \leq n$ e $\partial(b(x)) \leq n-m$ e portanto $\ell(nX) = n+1+(n-m+1) = 2n-m+2$.

Se $a_o \varepsilon k^2$, neste caso $X = v_1+v_2$, isto é, X é decomposto como $f = 2$ então $v_1(y) = v_2(y) = -m$.

Como no caso de $a_o \notin k^2$, estamos reduzidos a estudar $v_i(z)$ quando $z \varepsilon L(nX)$, $z = a(x)+yb(x)$ com $a(x)$, $b(x)$ pertencentes a $k(x)$ e $\partial a(x) = \partial b(x) + \frac{\partial f}{2}$.

Suponhamos $v_i(z) > \min\{v_i(a(x)), v_i(yb(x))\}$ para $i=1,2$. Para tanto precisamos $v_i(c_o+c'_o\, y/x^m) > 0$ para cada i, temos $h_i(c_o+c'_o\, y/x^m) = 0$ e daí $c_o = -c'_o\, h_i(y/x^m)$.

Como $h_1(y/x^m) = a$ e $h_2(y/x^m) = -a$, temos $c_o = -c'_o\, a$ e $c_o = c'_o a$ e assim $2c_o = 0$. Sendo a característica de $k \neq 2$ temos que $c_o = 0$, o que é um absurdo. Logo $v_i(c_o \neq c_o\, y/x^m) = 0\ \forall_i$, $i = 1,2$, e isto nos mostra que $v_i(z) = -s$, isto é, $v_i(z) = \min\{v_i(a(x)), v_i(yb(x))\}$. E daí $\ell(nX) = 2n-m+2$.

Em Resumo:

(i) Se grau de f é ímpar $\ell(nX) = 2n-m+2$

(ii) Se grau de f é par $\ell(nX) = 2n-m+2$

2.6.3. - Teorema

Sejam k um corpo de característica $\neq 2$ e $K = k(x,y)$ um corpo de funções algébricas de uma variável sobre k, tal que $y^2 = f(x)$, $f \in k[x]$ é um polinômio livre de quadrados.

Se g é o gênero de K. Então

$g = \left[\frac{\partial f-1}{2}\right]$ ([ ]: é a função menor inteiro)

Demonstração

Se $\partial f = 2m+1$, $m \in \mathbb{Z}_+$, então $\ell(nX)=2n-n+1$. Para $n > 2g-2$, o teorema de Riemann-Roch nos dá $\ell(nX)=d(nX)-g+1$. Logo $2n-m+1=d(nX)-g+1=2n-g+1$. Daí $m=g$.

Se $\partial f = 2m$, $m \in \mathbb{Z}$, $m \geq 1$, temos $\ell(nX)=2n-m+2$. Para $n \geq 2g-2$, pelo teorema de Riemann-Roch temos $\ell(nX) = 2n-g+1$. Assim, $2n-m+2 = 2n-g+1$, logo $g \geq m-1$.

Dos dois casos concluimos que $g = \left[\frac{\partial f-1}{2}\right]$.

∎

3 - CORPOS DE GÊNERO ZERO

3.1. - Preliminares

Neste Capítulo caracterizamos os corpos de gênero zero.

3.2. - Corpos de Gênero Zero

3.2.1. - Teorema

Toda extensão transcendente pura, $k(x)$ de k é de gênero zero.

Demonstração

Seja v_∞ a valorização infinita de $k(x)$ e consideremos o espaço $\mathcal{L}(nv_\infty) = \{y \in k[x];\ (y) \geq -nv_\infty\}$. Se $y \in L(nv_\infty)$, então $v_\infty(y) \geq -n$ e $v(y) \geq 0$ para toda valorização v de $k(x)|k$, $v \neq v_\infty$. Como $v_\infty(y) = -\partial y$ e $y \in k[x]$, temos que $L(nv_\infty)$ é o subespaço vetorial de $k[x]$, formado pelos polinômios $y \in k[x]$ tais que $\partial y \leq n$. Uma base para $L(nv_\infty)$ sobre k é $\{1, x, x^2, \ldots, x^n\}$ e daí a dimensão de $L(nv_\infty)$ é $n + 1$.

Se tomarmos $n > 2g-2$ temos $i(nv_\infty) = 0$ e pelo Teorema de Riemann-Roch, $\ell(nv_\infty) = d(nv) - g+1$. Como $d(nv_\infty) = n$, temos $n+1 = n-g+1$ daí $g = 0$.

■

3.2.2. - Teorema

Todo corpo K de gênero zero, admite uma valorização,

bre k de grau 1 ou 2.

Demonstração

Seja $E = \{d(X);\ X \in \mathrm{Div}\, K|k\}$. Assim E é um ideal de $\mathbb{Z}$ e portanto principal. Logo existe um inteiro $d>0$ tal que $E = d\mathbb{Z}$

Sendo o grau de um divisor canônico C igual a 2g-2 e como $g = 0$, temos que $2 \in d\mathbb{Z}$, isto é, d divide $\mathbb{Z}$, logo $d = 1$ ou $d = 2$.

Consideremos X um divisor de grau d. Pela desigualdade de Riemann-Roch, $\ell(X) > d(X) - g + 1 > 2$, e portanto $L(X)$ não é formado apenas por constantes, isto é, existe $y \in L(X)_1$ $y \notin k$. Neste caso $(y) \geq -X$. Assim o divisor $Y = X + (y) > 0$, é positivo e de grau d.

Sejam Y um divisor positivo com grau d e v uma valorização que seja uma componente de Y. Como $Y \geq 0$, $v \leq Y$ e portanto $1 \leq d(v) \leq d(Y) = d$. Se $d = 1$ então $d(v) = 1$.

Se $d = 2$ temos $d(v) = 1$ ou $d(v) = 2$, De qualquer modo $d(v) = 1$ ou $d(v) = 2$. ∎

3.2.3. - Teorema

Um corpo K, admitindo uma valorização de grau 1 tem gênero zero se, e somente se, K é racional.

Demonstração

Consideremos v uma valorização de K|k tal que $d(v) = 1$. Da desigualdade de Riemann-Roch $\ell(v) \geq d(v) - g + 1 = 2$, pois

$g = 0$. Portanto existe na função não constante $x \in L(v)$, tal que $(x) \geq -v$. Assim $(x)_\infty = v$ e como

$$d((x)_\infty) = [K:k(x)] = d(v) = 1, \quad K = k(x)$$

A reciproca é trivial pelo teorema 3.2.1. ∎

3.2.3.1. - Corolário

Seja K um corpo de gênero zero. K é racional se, somente se, existe um divisor de grau ímpar.

Demonstração

Basta mostrar que a existência de um divisor de grau ímpar implica na existência de um divisor de grau 1.

Sejam D um divisor de grau ímpar, digamos $d(D) = 2n+1$, $n \in \mathbb{Z}$ e C um divisor canônico. Como C tem grau -2, temos que $D+(nC)$ é um divisor de grau 1.

3.2.4. - Teorema

Todo corpo K de característica diferente de dois e de gênero zero é da forma $K = k(x,y)$, onde x,y estão relacionados pela equação $y^2 = ax^2 + b$, $a, b \in k$, $a \neq 0$.

Demonstração

Suponhamos que K admite uma valorização de grau 1. Então $K = k(t)$.

Basta considerar $x = y = t$ e $a = 1$ e $b = 0$ e mostramos que $K = k(x,y)$ com $y^2 = ax^2 + b$.

Suponhamos agora que $K|k$ admite valorização de grau dois. Seja v_p uma tal valorização. Como $d(v_p) = 2 > 2g-2 = -2$, temos pela fórmula de Riemann-Roch

$$\ell(v_p) = d(v_p) - g + 1 = 3.$$

Seja $\{1,u,t\}$ uma base de $L(v_p)$ sobre k. Então $(u) \geq -v_p \Leftrightarrow v_p(u) = -1$. Como $u \notin k$ então $(u)_\infty > 0$, portanto $(u)_\infty = v_p$. Assim $[K:k(u)] = 2$. De maneira análoga $[K:k(t)] = 2$ e $(t)_\infty = v_p$. Se $t \in k(u)$ então os polos de t estão sobre a valorização infinita de k(u) e portanto $t \in k[u]$.

Sendo $(t)_\infty = v_p$ isto nos mostra que $\partial(t) = 1$.

Assim podemos escrever $t = c_1u + c_2$ com $c_1, c_2 \in k$. Como u e t são k-linearmente independentes temos uma contradição. Assim t não pertence a k(u). Analogamente $u \notin k(t)$. Vemos assim que $[k(u,t):k(u)] \neq 1$ e como

$[K;k(u,t)] \cdot [k(u,t);k(u)] = [K:k(u)] = 2$, temos

$[K:k(u,t)] = 1$ daí $K = k(u,t)$.

Seja $f(U,T) \in k[U,T]$ um polinômio irredutível tal que $f(u,t) = 0$. Como t é de grau dois sobre k(u) e u é de grau dois sobre k(t) temos,

$$\partial_U(f) = \partial Tf = 2.$$

Assim, $f(U,T) = a_{0,0}U^2T^2 + a_{0,1}U^2T + a_{1,0}UT^2 + a_{0,2}U^2 + a_{11}UT +$

$$a_{2,0}T^2 + a_{1,2}U + a_{2,1}T + a_{22}.$$

com $a_{i,j} \varepsilon k$.

Suponhamos $a_{0,0} \neq 0$. Como $0 = f(u,t) = a_{0,0}u^2t^2 +$

$+ a_{1,0}u^2t + a_{0,1}ut^2 + a_{0,2}u^2 + a_{1,1}ut + a_{2,0}t^2 + a_{1,2}u + a_{2,1}t +$

$+ a_{2,2}$.

Temos:

$$(*)\ -a_{000}u^2t^2 = a_{1,0}u^2t + a_{0,1}ut^2 + a_{,02}u^2 + a_{1,1}ut + a_{2,0}t^2 +$$

$$a_{1,2}u + a_{2,1}t + a_{22}.$$

Aplicando v_p a(*) temos $-4 \geq -3$ o que é um absurdo, logo $a_{0,0}=0$.

Suponhamos agora que $a_{0,1} \neq 0$ e que $a_{1,0} \neq 0$. Podemos então escrever $v_p[ut(a_{0,1}u + a_{1,0}t)] \geq -2$ e daí $v_p(a_{0,1}u + a_{1,0}t) \geq 0$.

Como $a_{0,1}u + a_{1,0}t \varepsilon L(v_p)$, então $(a_{0,1}u + a_{1,0}t) \geq -v_p$ e daí $V_q(a_{0,1}u + a_{1,0}t) \geq 0$ $\forall q \neq p$. Assim mostramos que $v(a_{0,1}u+a_{1,0}t) \geq 0$ para toda valorização v e daí $a_{0,1}u + a_{1,0}t \varepsilon k$. Existe, então $c \varepsilon k$ tal que $a_{0,1}u+a_{1,0}t = c$ o que contradiz a independência linear de 1,u e t. Portanto $a_{1,0} = a_{0,1} = 0$.

Suponhamos agora, $a_{2,0} = 0$. Temos então $a_{0,2}u^2 + a_{1,1}ut = u(a_{0,2}u+a_{1,1}t)$ daí $v_p|u(a_{0,2}u+a_{1,1}t)| > -1$, pelo argumento do parágrafo anterior temos $a_{0,2}u + a_{1,1}t \varepsilon k$ o que nos leva a um absurdo, porque contratia a independência linear de 1, u e t. Logo $a_{2,0} \neq 0$ e podemos então supor $a_{2,0} = 1$. Assim temos a equação.

$$(**)\ t^2+(a_{1,1}u+a_{2,1})t + a_{0,2}u^2 + a_{1,2}u + a_{2,2} = 0$$

Fazendo, $x = u+[(a_{1,1}a_{2,1}-2a_{1,2})/(a_{1,1}^2 - 4\,a_{0,2})]$

$$y = t+ [(a_{1,1}u + a_{2,1})/2]$$

$$a = (a_{1,1}^2 - 4a_{0,2})/4$$

$$b =[(a_{2,1}^2 - 4a_{2,2})-(a_{1,1}a_{2,1}-2a_{1,2}^2)/(a_{1,1}^2-4a_{0,2})]/4$$

e substituindo em (**) e observando que a característica de k é diferente de dois, obtemos

$y^2 = ax^2 + b$ com $a, b \in k$. Assim, concluimos que

$K = k(u,t) = k(x,y)$ ∎

Afirmação 2: Em um corpo K de gênero zero, todo divisor de grau zero é principal.

De fato, seja X um divisor de grau zero. Como $0 > -2$, pelo teorema geral de Riemann-Roch, $\ell(-X) = d(-X)-g+1 = 1$. Assim existe $x \in L(-X)-k$. Mas $x \in L(-X)$ se, somente se, $(x)-X \geq 0$. Como $(x)-X$ é um divisor positivo com grau zero, devemos ter $(x)-X = 0$, isto é, $(x) = X$. ∎

3.2.5. - Lema

Os elementos geradores de k(x) sobre k, são elementos da forma

$$y = \frac{a + bx}{c + dx} \quad , \quad ad - bc \neq 0$$

Demonstração

Seja K = k(x). Se y ε k(x) então y é da forma y = f(x)/g(x) com (f(x),g(x)) = 1. Se y é um gerador, então $[K:k(y)] = d((y)_\infty) = d((y)_0) = 1$.

Para efeito de raciocinio, suponhamos inicialmente que $\partial f \geq \partial g$ e v uma valorização tal que v(y) > 0.

Como v é equivalente a valorização v_o (p(x)-ádica) e sendo (f,g) = 1 temos v(g) = 0 e como v(y) = v(f)-v(g) e daí v(y) = v(f) > 0. Portanto $(y)_o = \sum_{v(y)>0} v(y).v = \sum_{v(f)>0} v(f).v =$ $= (f)_o$:

Como $(f) = \sum_v v(f)v = \sum_{v(f)>0} v(f)v + \sum_{v(f)<0} v_\infty(f).v_\infty$

$$(f) = (f)_o - \partial f v_\infty, \text{ então } (y)_o = (f) + \partial f v_\infty.$$

Sendo $(y)_o$ um divisor positivo de grau 1, temos que $1 = d((y)_o) = d((f)) + \partial f d(v)_\infty) = \partial f$. Logo $\partial f = 1$.

Considerando agora $\partial f \leq \partial g$ e usando o mesmo raciocínio para os polos de y temos

$(y)_\infty = - \sum_{v(y)<0} v(y)v$, sendo v(y)<0 e v(g)<0, mas

$$(y)_\infty = (1/y)_o = (g/f)_o = (y)_o.$$

Como $(g) = \sum_v v(g)v = \sum_{v(g)>0} v(g)v + \sum_{v(g)<0} v_\infty(g)v_\infty$

$(g) \geq (g)_o - \partial g v_\infty$ daí $(y)_\infty = (g) + \partial g v_\infty$, logo $\partial g = 1$. Assim $y = \frac{ax + b}{cx + d}$. Evidentemente $at-bc \neq 0$, pois $x \in k(y)$.

Reciprocamente, se $y = \frac{ax + b}{cx + d}$, $ad-bc \neq 0$

Se $b \neq 0$ $[K:k(y)] = d((y)_o) = d(a+bx) = \partial(a+bx) = 1$.
Se $b = 0$, temos $d \neq 0$ e $[K:k(y)] = d((y)_\infty) = \partial(c+dx) = 1$.
Portanto y é gerador. ∎

Consideremos $K = k(x,y)$, com $y^2 = ax^2+b$, $a \neq 0$ $a,b \in k$ e característica de K diferente de dois. Dizemos que o ponto $(x_o,y_o) \in k \times k$ é uma solução racional para $y^2 = ax^2 + b$ se $y_o^2 = x_o^2 + b$.

Se $b \in k^2$, o ponto $(0,\sqrt{b})$ é uma solução racional para $y^2 = ax^2 + b$.

A equação $x^2 + y^2 = 3$ sobre $\mathbb{Q}$ não possui solução racional. De fato, suponhamos que $\left(\frac{m}{n}, \frac{m_1}{n_1}\right)$ é uma solução de $x^2+y^2 = 3$ em $\mathbb{Q}$. Assim

$$\frac{m^2}{n^2} + \frac{m^2}{n_1^2} = 3$$

$$\frac{n_1^2 m^2 + n^2 . m_1^2}{n^2 . n_2^1} = 3$$

$$n_1^2 m^2 + n^2 m_1^2 = 3n^2 n_1^2$$

Efetuando, todas as possíveis simplificações, sem perda de generalidades, podemos considerar a,b e c inteiros positivos

dois à dois primos entre si, tais que.

(*) $a^2 + b^2 = 3c^2$

Se $a \equiv 0 \mod (3)$ então $3 \backslash a$ e $3 \backslash a^2$ pela equação (*) temos que $3 \backslash b^2$ e portanto $3 \backslash b$. Isto nos mostra que $3 \backslash c$. Logo a,b e c não são dois à dois primos.

Se $a \equiv 1 \mod(3)$ então $a^2 \equiv 1 \mod (3)$ e $b^2 \equiv 1 \mod(3)$. Como $b \not\equiv 0 \mod(3)$ então $b \equiv 1 \mod(3)$ ou $b \equiv 2 \mod(3)$. Sendo $b \not\equiv 0 \mod(3)$, logo $b \equiv 1 \mod(3)$ ou $b \equiv 2 \mod(3)$. Assim, temos qhe $a^2 \equiv 1 \mod(3)$ e $b^2 \equiv 1 \mod(3)$. Logo $a^2+b^2 \equiv 2\mod(3)$, daí $3c^2 \equiv 2 \mod(3)$ o que é um absurdo, pois, $3 \nmid 2$.

Assim $x^2 + y^2 = 3$ não tem ponto racional sobre Q.

3.2.6. - Lema

Sejam k um corpo com característica diferente, de dois e $K = k(x,y)$, com $y^2 = ax^2 + b$, um corpo de gênero zero. $K|k$ é racional se, somente se, a equação $y^2 = ax^2 + b$ tem solução em $k \times k$.

Demonstração

Suponhamos, inicialmente que $(x_o, y_o) \in k \times k$ seja uma solução racional da equação $y^2 = ax^2 + b$, $a \neq 0$, e a,b $\in k$.

Consideremos $u = x+x_o$ e $v = y+y_o$, logo $x = u-x_o$ e $y = v-y_o$. Substituindo estes valores em $y^2 = ax^2 + b$ obtemos

$$(v-y_o)^2 = a(u-x_o)^2 + b$$

$v^2 - 2vy_o + y_o^2 = au^2 - 2aux_o + ax_o^2 + b$

Como $y_o^2 = ax_o^2 + b$ temos que $v^2 - 2vy_o = au^2 - 2ax_o u$ e

$v^2 - 2y_o v + 2ax_o u + au^2 = 0$.

Dividindo esta última igualdade por u^2 temos:

$$\left(\frac{v}{u}\right)^2 - 2y_o \frac{v}{u^2} + \frac{2ax_o}{u} + a = 0$$

$\left(\frac{v}{u}\right)^2 - \left(2y_o \frac{v}{u} + 2ax_o\right) \frac{1}{u} + a = 0$. Assim temos que $1/u$ pode ser escrito como função de (v/u) isto é, $u \in k(u/v)$ o que acarreta $v \in v \in k(v/u)$. Estando $k(v/u) \subset k(u,v)$ e como $u,v \in k(u,y)$ temos $k(u,v) = k(v/u)$ daí $K = k(u,v)$ que é racional.

Reciprocamente, suponhamos K racional, isto é, $K = k(u)$.

Como $d((y)_\infty) = [K:k(y)] = 2$ temos que existe uma valorização v_p de grau 1 na qual y não tem polos, isto é $v_p(y) \geq 0$.

Sendo $v_p(y) \geq 0$ temos que $v_p(y^2) \geq 0$. Assim $v_p(y^2) = v_p(ax^2+b) \geq \min\{v_p(ax^2), v_p(b)\} \geq 0$ então

$v_p(ax^2) \geq 0 \Rightarrow v_p(x) \geq 0$. Logo $x,y \in A_{v_p}$, em K_{v_p} temos $\bar{y}^2 = a\bar{x}^2 + b$. Como $[K_{v_p}:k] = 1$ então $K_{v_p} = k$, havendo uma solução racional para a equação $y^2 = ax^2 + b$, a saber $(\bar{x},\bar{y})$.

■

Resumindo:

3.2.7. - Teorema

Um corpo K de funções algébricas de uma variável

tem gênero zero, se, somente se, ele é um dos seguintes tipos:

(i) K é um corpo de funções racionais, isto é, $K = k(x)$.

(ii) $K = k(x,y)$, um corpo de funções de uma cônica

$y^2 = ax^2 + b$, $a \neq 0$, $a, b \in k$.

Mais ainda um corpo do tipo (ii) se torna do tipo (i) se, somente se, a canônica contêm um ponto racional.

3.3. - Classificação dos Corpos de Gênero Zero

Neste Capítulo consideramos K um corpo de funções algébricas de uma variável sobre k, com característica de k diferente de dois. Indicamos por $\bar{k}$ o fecho algébrico de k.

Vamos apresentar uma melhora da equação da canônica ($y^2 = ax^2 + b$, $a, b \in k$) no caso em que $[\bar{k}:k]$ é finito e no caso de k ser finito.

3.3.1 - Teorema

Seja $K|k$ um corpo de gênero zero. se $1 < [\bar{k}:k] < \infty$, então K é racional ou é da forma $K = k(x,y)$ com $y^2+x^2+1 = 0$.

Demonstração

Como $1 < |\bar{k}:k| < \infty$, da teoria de Artin-Schreier temos $[\bar{k}:k] = 2$ e $\bar{k} = k(\sqrt{-1})$, k é real fechado e de característica zero. Além disso k é ordenado pelos elementos que são quadrados.

Fazendo a mudança de x por $\frac{b_1}{a_1}x$ e y por $b_1 y$, a equação $y^2 = ax^2 + b$ torna-se $y^2 + x^2 + 1 = 0$. De fato,

$$b_1^2 y^2 = a \left(\frac{b_1}{a_1}\right)^2 x^2 + b$$

$$b_1^2 y^2 = -a_1^2 \frac{b_1^2}{a_1^2} x^2 - b_1^2$$

$$b_1^2 y^2 = -b_1^2 x^2 - b_1^2 = b_1^2(-x^2-1)$$

$$y^2 = -x^2 - 1 \text{ daí } y^2 + x^2 + 1 = 0.$$

Como k é formalmente real, -1 não é soma de quadrados em k. Logo a equação $y^2 + x^2 + 1 = 0$ não tem solução racional em k^2. Portanto K não é racional. ■

Concluimos assim que quando $[\overline{k}:k] = 2$ há dois tipos de corpos de gênero zero que são; os corpos racionais e os corpos da forma $K = k(x,y)$ com $y^2 + x^2 + 1 = 0$.

Apresentaremos uma outra demonstração para o teorema 3.3.1.

A existência de um divisor de grau ímpar ou de solução racional para a equação $y^2 = ax^2 + b$, acarreta que K é um corpo racional. Assim basta analisar o caso em que a ε b não são quadrados.

Seja $x_o \in k - k^2$ e $x \in \overline{k}$, $x = \sqrt{x_o}$. Por argumento de grau, $\overline{k} = k(x)$. Se $y \in k - k^2$ então $\sqrt{y} \in \overline{k}$ e como $\overline{k} = k(x)$ temos:

Pela teoria de Kummer, (Cáp. 1, § 4), se tomarmos $B = k^*$ teremos a composição de todos os corpos $k(a^{1/m})$ $a \in B$ igual a $\bar{k}$, isto é, $K_B = \bar{k}$ e

$$[K_B:k]=[k:k]= (B:k^*)^2 = (k^*:k^{*2}) = 2$$

Assim, $k^*/k^{*2} = \{-\bar{1},\bar{1}\}$, isto é, um elemento não nulo de k, ou é quadrado ou seu simétrico é quadrado.

Como sabemos os corpos $K|k$ de funções algébricas de uma variável cujo gênero é zero e característica é diferente de dois caracterizam-se por serem da forma $K = k(x,y)$ com $y^2 = ax^2 + b$, $a \neq 0$, $a,b \in k$. Se b é quadrado o ponto $(0,\sqrt{b})$ é uma solução para $y^2 = ax^2+b$. Portanto K é racional (Veja Lema 3.2.6.).

No caso em que b não é quadrado, mas a é quadrado, substituindo x por 1/v em $y^2 = ax^2 + b$ obtemos:

$$y^2 = a\frac{1}{v^2} + b$$

$$(yv)^2 = a+bv^2.$$

Seja $yv = z$, assim $z^2 = a+bv^2$. Pelas condições anteriores, $K|k$ é racional. Assim, se a ou b for quadrado temos que K é racional.

Restamos analisar o caso em que a e b não são quadrados.

Se a e b não são quadrados, então podemos escrevê-los assim:

$$a = -a_1^2 \qquad e \qquad b = -b_1^2$$

$\sqrt{y} = y_0 + y_1 x$ com $y_0, y_1 \in k$, $y_1 \neq 0$, daí

$$y = y_0^2 + 2y_0y_1x + y_1^2x^2.$$

Sendo $x^2 = x_0 \in k$ e $y \in k$ o termo que contém x é nulo, além do mais, y_1 e x não são nulos. Logo $y_0 = 0$. Portanto, $y = y_1^2 x^2 = y_1x_0$. Então $y/x_0 = y_1^2$, isto é, $k\text{-}k^2=k^2x_0$, isto é, y/x_0 é um quadrado em k. Assim se a e b não são quadrados então a/x_0 e b/x_0 são quadrados e $a/b = \dfrac{a/x_0}{b/x_0}$ é um quadrado em k.

Efetuando a mudança de x por $\sqrt{\frac{b}{a}}\,u$ e y por $\sqrt{b/x_0}\cdot v$, em $y^2 = ax^2 + b$, com $a,b \in k\text{-}k^2$ obtemos:

$$(\sqrt{b/x_0})^2 v^2 = a(\sqrt{b/a})^2 + b$$

$$\frac{b}{x_0}v^2 = a\,\frac{b}{a}u^2 + b$$

$$v^2 = x_0u + x_0$$

Portanto no caso em que $[\bar{k}:k] = 2$ temos dois tipos de corpos de gênero zero, que são os racionais e os do tipo $K = k(x,y)$ com $y^2 = cx^2+c$, $\sqrt{c} \notin k$.

Se $\sqrt{-1} \in k$, a equação $y^2 = c(x^2+1)$ tem ponto racional e portanto K é racional.

Se $\sqrt{-1} \notin k$, podemos tomar $x = -1$ e a equação $y^2 = ax^2 + b$ torna-se $y^2 + x^2 + 1 = 0$ que tem ponto racional se -1 é soma de quadrados.

No caso de $k = \mathbb{R}$ (corpo dos reais) há dois tipos de corpos de funções de gênero zero, que são os racionais e os do tipo $\mathbb{R}(x,y)$ com $y^2+x^2 + 1 = 0$ que é não racional.

Vamos agora classificar os corpos de gênero zero quando k é um corpo finito. Para tanto faremos uso das seguintes observações:

Observação 1: Sejam $F = F_q$ corpo finito com característica q, e $L = F_q^n$ uma extensão de grau n de F_q se $\xi \in F_q^{*n}$, $\xi \neq 1$, então $\xi^{\frac{q^n-1}{q-1}}$ é gerador de F_q^*.

Observação 2:

$(q-1)$ e $(q^n-1)/(q-1)$ são primos entre si.

De fato, se $(q^n-1)/(q-1)$ não fosse primo com $(q-1)$, então $\frac{q^n-1}{q-1}$ geraria um subgrupo de F_q^* com cardinalidade

$$\frac{q-1}{\text{M.D.C.}\{(q-1);(q^n-1)/(q-1)\}}$$

Como $\xi^{\frac{q^n-1}{q-1}}$ gera F_q^*, então $\text{M.D.C.}\{q-1,(q^n-1)/(q-1)\} = 1$.

Seja E uma extensão finita do corpo K. Para $\alpha \in E$, seja $\alpha_L \in \text{Hom}_K(E,E)$ a K-transformação linear induzida no espaço vetorial E sobre K pela multiplicação à esquerda por α, isto é, $\alpha_L(\beta) = \alpha.\beta$, $\beta \in E$.

Define-se a Norma de E sobre K como sendo a aplicação

$$N_{E|K} : E \to K$$
$$\alpha \to N_{E/K}(\alpha) = \det(\alpha_L), \quad \alpha \in E$$

Onde $\det(\alpha_L)$ é o determinante da matriz associada à transformação linear α_L em relação a uma base de E sobre K.

Exemplo 1: Considere $\mathbb{Q}(i)$, onde $\mathbb{Q}$ é o corpo dos racionais e $i^2 = -1$. O elemento $(x+iy) \in \mathbb{Q}(i)$ com x e y $\in \mathbb{Q}$, induz, pela multiplicação à esquerda, a $\mathbb{Q}$-transformação linear de $\mathbb{Q}(i)$, cuja matriz em relação a base $\{1,i\}$ de $\mathbb{Q}(i)$ e

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

Portanto, $N_{\mathbb{Q}(i)|\mathbb{Q}}(x+iy) = x^2+y^2$.

Notemos que $N_{E/K}(\alpha.\alpha') = N_{E/K}(\alpha).N_{E/K}(\alpha')$

3.3.2. - Definição

Seja E uma extensão algébrica de um corpo K, e seja o corpo $E_s = \{\alpha \in E;\ \alpha$ é separável sobre $K\}$. O grau de separabilidade de E sobre K é o índice $[E_s:K]$ e o de iseparabilidade de $[E:E_s]$.

3.3.3. - Teorema

Sejam $L \supset E \supset K$, corpos, onde L é algebricamente fechado e $[E:K] = n$. Sejam $n_s = [E_s:K]$ e $n_i = [E:E_s]$ e $\sigma_1, \sigma_2, \ldots, \sigma_{n_s}$ K-isomorfismos distintos de E em L.

Então para cada $\alpha \in L$

$$N_{E/K}(\alpha) = \left[\prod_{t=1}^{n_s} \sigma_t(\alpha) \right]^{n_i} . \quad \text{(Veja [L].)}.$$

■

Se E, K são dois corpos finitos, $K \subset E$ a função norma é sobrejetiva.

De fato, consideremos $K = F_q$ e $E = F_q^n$ uma extensão de grau n de K. Como o grupo de Galois de E sobre K é gerado pelo automorfismo $\psi: E \to E$ tendo K como corpo fixo.

$$x \to x^q$$

Assim, se ξ é um gerador de E^*, a norma de ξ é

$N(\xi)_{E/K} = \xi . \xi^q . \xi^{q^2} \ldots \xi^{q^{n-1}} = \xi^{\frac{q^n-1}{q-1}} \in K$ é também um gerador de K^*. Portanto a norma é sobrejetiva, pois transforma gerador em gerador.

3.3.4. - Teorema

Seja K um corpo de funções algébricas uma variável sobre K, de gênero zero e característica de k, $\neq 2$. Se k é um corpo finito, então K e um corpo racional.

Demonstração

Como K é um corpo de gênero zero e de característica, $\neq 2$, K caracteriza-se por ser da forma $K = k(x,y)$ com $y^2 = ax^2 + b$, $a \neq 0$, $a,b \in k$. Se a ou b são quadrados então K é racional.

Resta-nos mostrar a existência de solução em k^2 para a equação $y^2 = ax^2 + b$ com a e b não quadrados.

De $y^2 = ax^2 + b$ obtemos $b = y^2 - ax^2$.

No corpo $k(\sqrt{a})$ temos

$$b = y^2 - ax^2 = (y+\sqrt{a}x)(y-\sqrt{a}x) = N_{k(\sqrt{a})|k}(y+\sqrt{a}x)$$

Logo $b = N_{k(\sqrt{a})|k}(y+\sqrt{a}x)$. Como N é sobrejetiva então a equação $y^2 = ax^2+b$, $a,b \notin k^2$ tem uma solução racional.

■

REFERÊNCIAS BIBLIOGRÁFICAS

[AM] M.F.Atiyah,I.G.Macdonald - Introduction to commutative Algebra. Addison Wesley, 1969.

[B] N. Bourbaki - Algèbre. Wesley Paris, Hermann, 1954.

[C] C.Chevalley - Introduction to the Theory of Algebraic. Functions of One Variable. New York, Amer.Math.Soc.1951.

[E] Otto Endler - Valuation Theory. Berlin,Springer Verlag, 1972.

[F] J.B. Fraleigh - A First Cours in Abstract Algebra. Addison Wesley, 1967.

[J] Nathan Jacobson - Lectures in Abstract Algebra. Princeton, D. Van. Nortrand, Company 1951-64.

[L] Serge Lang - Algebra. Addison Wesley, 1965.

[N] Herminio Borges Neto - Notas de Classificação de Corpos de Gênero Zero. Fortaleza-UFC - 1982.

[O] Karl Otto - Notas de aula sobre corpos de Funções Algébricas. Rio de Janeiro, IMPA, 1985.

[P] Alexander Prestel - Lectures on Formally Real Fields. Rio de Janeiro, IMPA (Monografias de Matemática 22).

[S] P. Samuel - Corps de Functions Algebrique. Rio de Janeiro, IMPA, 1963. (Notas de Matemática nº 28).

$[Z,S]_1$ O. Zarishi e P.Samuel - Commutative Algebra Vol. I - Princeton, D.Van Nostrand Company, 1959.

$[Z,S]_2$ O.Zarishi e P.Samuel - Commutative Algebra Vol. II 1960.