UMA PROVA ELEMENTAR DA HIPÓTESE DE RIEMANN PARA CURVAS ALGÉBRICAS SOBRE CORPOS FINITOS

Paulo Agozzini Martin

DISSERTAÇÃO APRESENTADA AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA OBTENÇÃO DO GRAU DE MESTRE
EM
MATEMÁTICA
ÁREA DE CONCENTRAÇÃO: ÁLGEBRA
ORIENTADOR:
Prof. Dr. WALTER RICARDO FERRER

Durante a elaboração deste trabalho o autor recebeu apoio financeiro da
FAPESP

São Paulo, abril de 1986

ÍNDICE

INTRODUÇÃO

Um dos problemas centrais da teoria dos números é o da solubilidade de equações diofantinas. E uma das técnicas elementares mais utilizadas no ataque de questões diofantinas, pela sua simplicidade e eficácia, é a de procurar soluções módulo p. Consideremos, por exemplo, a equação

$$y^2 = x^3 - x - 1$$

onde procuramos encontrar soluções inteiras. Se pensarmos nessa equação módulo 3, é claro que o lado esquerdo só pode ser 0 ou 1 (mod 3), enquanto o lado direito é -1 (mod 3), e portanto essa equação não possui soluções inteiras.

Ao estudar as soluções de uma congruência

$$f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{p}$$

é natural considerar soluções também nas extensões finitas $\mathbf{F}_p m$ de $\mathbf{F}_p$. Buscando condensar toda a informação diofantina, Artin, [1], introduziu em 1924 a função zeta de uma variedade algébrica X sobre um corpo finito $\mathbf{F}_q$:

$$Z(X/\mathbf{F}_q;\ t) = \exp\left(\sum_{m \geq 1} N_m \frac{t^m}{m}\right)$$

onde N_m é o número de soluções de X com coordenadas em $\mathbf{F}_q m$. De fato, Artin utilizava a linguagem de corpos de funções algébricas de uma variável e definiu a função zeta por analogia com a função zeta de um corpo de números algébricos. E foi também Artin que formulou a "hipótese de Riemann" para a função zeta: os zeros de $Z(X/\mathbf{F}_q;\ q^{-s})$ estão todos na reta $Re(s) = 1/2$. (Fizemos a mudança de variável $t = q^{-s}$).

Foi somente em 1931 que F.K.Schmidt, [7], mostrou que o teorema de Riemann-Roch podia ser usado para provar que a função zeta de uma curva $X/\mathbb{F}_q$ de gênero g é uma função racional de $t = q^{-s}$, da forma:

$$\zeta(s) = \frac{P(q^{-s})}{(1-q^{-s})\ (1-q^{1-s})}$$

onde $P(t) = \prod_{i=1}^{2g} (1-\alpha_i t)$ é um polinômio de grau 2g com coeficientes em $\mathbb{Z}$ e tal que a aplicação $\alpha \to q/\alpha$ é uma permutação do conjunto das raízes de P(t). Em termos da variável complexa s, isso quer dizer que $P(q^{-s})$ satisfaz uma equação funcional sob a troca $s \to 1 - s$.

A "hipótese de Riemann" em termos dos α_i fica:

$$|\alpha_i| = q^{1/2}$$

Tomando o logarítmo em ambos os lados da igualdade abaixo:

$$\exp\left(\sum_{m\geq 1} N_m \frac{t^m}{m}\right) = \frac{\prod_{i=1}^{2g} (1-\alpha_i t)}{(1-t)\ (1-qt)}$$

obtemos:

$$N_m = 1 + q^m - \sum_{i=1}^{2g} \alpha_i{}^m$$

que é precisamente o número de soluções da curva X na extensão $\mathbb{F}_q m/\mathbb{F}_q$.

Assumindo a "hipótese de Riemann" $|\alpha_i| = q^{1/2}$, obtemos imediatamente da expressão acima:

$$|N_m - 1 - q^m| \leq 2g\, q^{m/2}$$

E Hase, [5], observou que a desigualdade acima implica, por sua vez a "hipótese de Riemann".

Ou seja, no caso de curvas algébricas, a "hipótese de Riemann" é equivalente a uma desigualdade puramente diofantina.

O primeiro caso em que a "hipótese de Riemann" foi verificada foi provado por Gauss, [4], para a curva $y^2 = x^4 - 1$. Artin estabeleceu alguns outros casos particulares, e em 1933 Hasse provou o resultado para uma curva elíptica arbitrária.

Foi somente em 1940 que Weil, [8], provou a "hipótese de Riemann" para curvas de gênero arbitrário.

Num artigo bem conhecido de Weil, de 1949, ele conjecturou o que deveria ser verdadeiro para variedades de dimensão maior. Seja X uma variedade projetiva não singular de dimensão n sobre $\mathbb{F}_q$. Então:

(1) $Z(X/\mathbb{F}_q;\ t)$ é uma função racional de t.

(2) $$Z(X/\mathbb{F}_q;\ t) = \frac{P_1(t)\ P_3(t)\ \ldots\ P_{2n-1}(t)}{P_0(t)\ P_2(t)\ \ldots\ P_{2n}(t)}$$ onde

$$P_i(t) = \prod_{j=1}^{b_i} (1-\alpha_{ij}t), \quad \text{com} \quad |\alpha_{ij}| = q^{i/2}$$

(A última igualdade é a "hipótese de Riemann" nesse contexto).

(3) Sob a aplicação $\alpha \to q^n/\alpha$ os α_{ij} são levados bijetivamente nos $\alpha_{2n-i,j}$.

(4) No caso de X ser a "redução módulo p" de uma variedade projetiva não singular **X** em característica zero, então b_i é o i-ésimo número de Betti de **X**.

Essas são as famosas "conjecturas de Weil", que foram o impulso básico da Geometria Algébrica por mais de 20 anos. A história das tentativas que se fizeram para provar essas "conjecturas" é extremamente interessante, porém nos levaria longe demais. O leitor interessado pode consultar o artigo de Katz, [6], para uma boa resenha. Diremos somente que o análogo da "hipótese de Riemann" para dimensão arbitrária foi provado por Deligne, [3], em 1973, e a prova é extraordinariamente difícil. Mesmo a prova dada por Weil no caso de curvas de gênero arbitrário é difícil, e é considerada uma de suas maiores realizações.

Porém em 1973 Bombieri (baseado em trabalhos de Stepanov) deu uma demonstração da "hipótese de Riemann" para curvas que é "elementar", no sentido de que se utiliza somente do teorema de Riemann-Roch.

A idéia de Stepanov é simples: dada uma curva projetiva não singular $\mathbf{C}$ de gênero g sobre $\mathbf{F}_q$, procura-se uma função racional f definida em $\mathbf{C}$, não nula, que tem um zero de ordem $\geq m$ em cada um dos pontos $\mathbf{F}_q$-racionais de $\mathbf{C}$, exceto possivelmente num conjunto fixo de m_o pontos racionais de $\mathbf{C}$. Decorre então que

$$m(N_1 - m_o) \leq \#(\text{zeros de } f) = \#(\text{polos de } f)$$

e portanto

$$N_1 \leq m_0 + \frac{\#(\text{polos de } f)}{m}$$

Assim, se construirmos f com poucos polos teremos uma boa limitação para N_1.

A presente dissertação objetiva precisamente apresentar a prova da "hipótese de Riemann" para curvas segundo a versão de Bambieri-Stepanov, [2]. Embora o artigo de Bombieri tenha somente 3,5 folhas e fizéssemos o esforço para dar uma apresentação autocontida, isso não foi possível devido à natureza complexa do problema e aos muitos pré-requisitos que ele exige. Minimizamos a utilização de álgebra comutativa, procurando sempre que possível o enfoque geométrico, e na parte concernente a geometria algébrica, nos limitamos à definição clássica de variedade algébrica, cuja teoria está concentrada basicamente no mullstellensatz. Não pudemos, porém, evitar o uso de alguns resultados básicos da teoria das valorizações acerca de extensões de valorizações que não demonstramos no texto, mas que são encontráveis em qualquer livro de números algébricos.

Procuramos dar uma independência relativa aos capítulos para facilitar a leitura daqueles que não necessitarem de muitos requisitos básicos.

REFERÊNCIAS

[1] - E. Artin. Quadratische Körper en Gebiete der höheren Kongruenzen I, II, in Collected Papers, Springer-Verlag.

[2] - E. Bombieri. Counting points on curves over finite fields. Séminaire Bourbaki 1972/1973 nº 430.

[3] - P. Deligne. La conjecture de Weil I, II, Publ. Math. IHES 43 (1974) 273-307.

[4] - C.F. Gauss. Werke. (a) vol I pp.445-449
(b) vol II pp.67-92.

[5] - H. Hasse. Uber dil Kongruenzetafunctionen, Sitz-ber. d.Preuss. Akad. d. Wiss. 1934.

[6] - N. Katz. An overview of Deligne's proof of the Riemann Hypothesis for varieties over finite fields. Proccedings of Symposia in Purle Math. vol.28, 1976.

[7] - F.K. Schmidt. Analytische Zahlentheorie in Körpern der Characteristik p. Math. Zeit. 33 (1931). 1 - 32.

[8] - A. Weil. Sur les courbes algébriques e les varietés qui s'en déduisent. Hermann, Paris, 1948.

CAPÍTULO I

PRELIMINARES ALGÉBRICOS

Neste capítulo vamos enunciar os principais resultados da teoria dos corpos finitos e das valorizações, principalmente para que a exposição que se segue fique o mais autocontida possível. Como os resultados e teoremas são na sua maior parte elementares e podem ser encontrados em qualquer texto introdutório de álgebra (por exemplo: S. Lang, Algebra), não os demonstraremos aqui.

§1 - Corpos finitos

Se F é um corpo finito de q elementos, então é claro que F tem característica $p > 0$, e portanto pode ser considerado uma extensão de $\mathbf{Z}_p$, o corpo dos inteiros módulo p. Assim podemos pensar em F como um $\mathbf{Z}_p$-espaço vetorial e portanto $q = p^n$ para algum inteiro $n \geq 1$. Ou seja, se F é um corpo finito com q elementos então q é uma potência de certo primo p. Consideremos agora o problema inverso, a saber: dado $q = p^n$, para um primo p e um inteiro $n \geq 1$, achar um corpo finito que tenha exatamente q elementos.

PROPOSIÇÃO 1. Se n é um inteiro ≥ 1 e p um primo, existe um corpo finito com p^n elementos, univocamente determinado como subcorpo de um fecho algébrico $\overline{\mathbf{Z}}_p$. Além disso esse corpo é o corpo de decomposição do polinômio $x^{p^n} - x$ sobre $\mathbf{Z}_p$ e seus elementos são as raízes desse polinômio.

Em geral, denotaremos por $\mathbf{F}_q$ um corpo finito com q elementos. Se m e n são inteiros ≥ 1 então decorre da proposição 1 a

PROPOSIÇÃO 2. A inclusão $\mathbf{F}_q n \subset \mathbf{F}_q m$ equivale à n|m (n divide m).

Se k é um corpo finito com q elementos o grupo multiplicativo k^* de k é comutativo e tem ordem (q-1). Além disso, é bem conhecida a seguinte proposição:

PROPOSIÇÃO 3. O grupo multiplicativo k^* de k é cíclico de ordem q-1.

Seja $\mathbf{F}_q$ um corpo finito com $q = p^n$ elementos e consideremos a aplicação $\phi: \mathbf{F}_q \to \mathbf{F}_q$ dada por $x \to x^p$. Então ϕ é um automorfismo de $\mathbf{F}_q$, e é chamado automorfismo de Frobenius de $\mathbf{F}_q/\mathbf{F}_p$. Note-se que ϕ deixa $\mathbf{F}_p$ fixo, isto é, $\phi(x) = x$ para todo x de $\mathbf{F}_p$. Da teoria de Galois decorrem as duas proposições abaixo:

PROPOSIÇÃO 4. O grupo dos automorfismos de $\mathbf{F}_q$ é cíclico de ordem n, gerado pelo automorfismo de Frebenius de $\mathbf{F}_q/\mathbf{F}_p$, $x \to x^p$.

PROPOSIÇÃO 5. Seja k um corpo finito com q elementos e K/k é uma extensão finita de grau m. Então K/k é uma extensão de Galois cujo grupo de Galois é cíclico gerado pelo automorfismo de Frobenius de K/k, $x \to x^q$.

É útil considerar a seguinte caracterização explícita do fecho algébrico $\overline{\mathbf{F}_q}$ de um corpo finito $\mathbf{F}_q$ com q elementos. Consideremos a torre de corpos

$$\mathbf{F}_q \subset \mathbf{F}_{q^2} \subset \mathbf{F}_{q^{2\cdot 3}} \subset \ldots \subset \mathbf{F}_q m! \subset \mathbf{F}_q(m+1)! \subset \ldots \subset H$$

onde $H = \bigcup_{n \geq 1} \mathbf{F}_q n!$. É imediata a:

PROPOSIÇÃO 6. Se $\mathbb{F}_q$ é um corpo finito com q elementos então

$$\overline{\mathbb{F}_q} = \bigcup_{n \geq 1} \mathbb{F}_{q^{n!}}$$

e portanto a extensão $\overline{\mathbb{F}_q}/\mathbb{F}_q$ é de Galois.

É interessante observar que se $\sigma \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ então $\sigma(\mathbb{F}_{q^{m!}}) = \mathbb{F}_{q^{m!}}$, ou seja, a restrição de σ à $\mathbb{F}_{q^m}$ pertence à $Gal(\mathbb{F}_{q^{m!}}/\mathbb{F}_q)$. Essa simples observação será usada no §3 do Cap. II e no Cap. IV.

§2 - Valorizações discretas

DEFINIÇÃO. Seja K um corpo. Uma aplicação v definida no conjunto K^* dos elementos não nulos de K e tomando valores em $\mathbb{Z}$ diz-se uma valorização discreta de K se:

(a) $v(a.b) = v(a) + v(b)$

(b) v é sobrejetora

(c) $v(a+b) \geq \min\{v(a), v(b)\}$

É cômodo definir $v(0) = +\infty$ e considerar v extendida a K. Vamos reunir num lema as consequências imediatas da definição:

LEMA 1. Seja v uma valorização discreta de um corpo K e sejam $A_v = \{a \in K : v(a) \geq 0\}$ e $M_v = \{a \in K : v(a) > 0\}$. Então

(a) $v(1) = 0$; $v(a^{-1}) = -v(a)$

(b) $v(-1) = 0$; $v(-a) = v(a)$

(c) Se $v(a) \neq v(b)$ então $a + b \neq 0$ e

$$v(a+b) = \min \{v(a), v(b)\}$$

(d) A_v é um domínio de ideais principais de K cujo corpo de frações é K.

(e) M_v é o único ideal primo de A_v.

O anel A_v é chamado o anel da valorização discreta v e o ideal M_v é chamado o ideal maximal da valorização v. O corpo A_v/M_v é chamado de corpo de restos da valorização discreta v. Em geral, um anel comutativo com unidade A é chamado de anel de valorização discreta se existir um corpo K e uma valorização discreta v de K tal que $A = A_v$. O seguinte lema é uma útil caracterização dos anéis de valorização discreta (para uma prova ver Serre, Corps Locaux):

LEMA 2. Seja A um anel comutativo. Para que A seja um anel de valorização discreta é necessário e suficiente que A seja um anel local noetheriano e que seu ideal maximal seja gerado por um elemento não nilpotente.

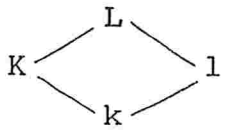
O próximo lema nos dará uma importante propriedade dos anéis de valorização discreta, que será utilizada adiante:

LEMA 3. Seja K um corpo e v uma valorização discreta de K. Então A_v é um subanel maximal de K.

Vamos agora enunciar os teoremas mais importantes sobre extensões de valorizações, que serão utilizados nos capítulos III e IV. Como nesses capítulos estaremos interessados unicamente em corpos de funções algébricas de uma variável, vemos desde já nos situar nesse contexto.

DEFINIÇÃO. Seja k um corpo arbitrário. Um corpo de funções algébricas de uma variável sobre k é um corpo K contendo k e verificando a condição: K contém um elemento x transcendente sobre k e $K/k(x)$ é uma extensão finita. O fecho algébrico de k em K, k', é chamado corpo de constantes de K, e é claro que K é um corpo de funções algébricas de uma variável sobre k'.

DEFINIÇÃO. Seja K um corpo de funções algébricas de uma variável com corpo de constantes k. Uma extensão de K é um corpo de funções algébricas de uma variável L, com corpo de constantes l tal que $L \supset K$ e $l \cap K = k$.



Seja então L/l uma extensão de K/k e w uma valorização discreta de L trivial sobre l. Se $w(x) = 0$ para todo $x \in K$ w diz-se trivial sobre K. Se esse não for o caso, a imagem $w(K) \subset \mathbf{Z}$ é um subgrupo de $\mathbf{Z}$ da forma $e\mathbf{Z}$ para certo inteiro positivo $e = e_{L/K}(w)$. É claro que $v = \frac{w}{e_{L/K}(w)}$ é uma valorização discreta de K trivial sobre k.

O inteiro $e = e_{L/K}(w)$ é chamado índice de ramificação de w sobre K, e a valorização w é dita uma extensão da valorização v.

É fácil ver que $A_w \cap K = A_v$ e $M_w \cap K = M_v$, e assim existe uma injeção canônica:

$$K_v = A_v/M_v \to A_w/M_w = L_w$$

e vale o seguinte lema:

LEMA 4. Seja L/l uma extensao de K/k. Então são equivalentes:

(a) $[l:k] < \infty$

(b) $[L:K] < \infty$

(c) $[L_w:K_v] < \infty$

Para uma prova ver Deuring, Lectures on the Theory of Algebraic Functions of One Variable, pg 93. O inteiro $[L_w:K_v] = d_{L/K}(w)$ é chamado o grau de w sobre K.

PROPOSIÇÃO 1. Seja K/k um corpo de funções algébricas sobre o corpo de constantes k, e v uma valorização discreta de K, trivial sobre k. Então $[K_v:k] < \infty$. (Ver Deuring, Idem pg 15).

Se L/l é uma extensão de K/k, é fácil ver que as condições abaixo são equivalentes:

(a') l/k é algébrica

(b') L/K é algébrica

(c') L_w/K_w é algébrica

Assim, se L/l extende K/k, diremos que se trata de uma extensão algébrica se for verificado um dos três itens acima, e diremos que é uma extensão finita se se verificar um dos itens do lema 4.

É importante observar que se L/l é uma extensão algébrica de K/k, então não existe nenhuma valorização discreta w de L que seja trivial sobre K. Pois se w fosse trivial em K, seja $\alpha \in L$, e seja $f(x) \in L[x]$ o polinômio irredutível de α sobre K:

$$f(\alpha) = \alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0 \quad , \quad a_i \in K$$

Então

$$0 = w(a_n) = w(\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha)$$

Se $w(\alpha) > 0$, pelo item (c) do lema 1 deste paragrá fo, então

$$w(\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha) = \min \{w(\alpha^n), \ldots, w(\alpha)\} = w(\alpha)$$

donde obtemos uma contradição.

TEOREMA 1. Seja L/l uma extensão qualquer de k/k. Se v é uma valorização discreta de K, trivial sobre k, o número de todas as possíveis extensões de v à valorizações discretas de L, triviais sobre l, é finito e positivo. (Ver Deuring, Idem, pg 96).

No teorema 2 abaixo vamos considerar o caso impor tante de extensões de Galois.

TEOREMA 2. Seja L/l uma extensão de Galois de K/k e v uma valorização discreta de K , trivial sobre k. Seja w uma ex tensão de v à L. Então qualquer extensão de v à L estará no conjunto $\{w \circ p : p \in Gal(L/K)\}$.

Para uma prova desse teorema no caso de extensões L/K finitas ver Deuring, Idem, pg 101. Para o caso geral ver O. Endler, Valuation Theory, pg 109.

TEOREMA 3. Seja L/l uma extensão finita de K/k. Seja v uma valorização discreta de K trivial em k, e sejam $w_1, \ldots, w_h$ todas as extensões de v a L. Então

$$[L:K] = \sum_{i=1}^{h} d_{L/K}(w_i)\, e_{L/K}(w_i)$$

Se, além disso a extensão for de Galois, então $d_{L/K}(w_1) = \ldots = d_{L/K}(w_h) = d$ e $e_{L/K}(w_1) = \ldots = e_{L/K}(w_h) = e$ e portanto

$$[L:K] = h\,d\,e$$

Para uma demonstração ver Iyanaga, Theory of Numbers, pg 138.

O lema seguinte é extremamente importante para o que se segue:

LEMA 5. Se L/l é uma extensão algébrica separável de K/k e tal que L = Kl então toda valorização discreta w de L, trivial sobre l, tem índice de ramificação $e_{L/K}(w) = 1$, sobre K. (Ver Deuring, pg. 113).

Assim a restrição w/k será uma valorização discreta de K trivial sobre k.

CAPÍTULO II

INTRODUÇÃO À GEOMETRIA ALGÉBRICA

§1 - Variedades afins

A geometria algébrica clássica trata do estudo geométrico do conjunto das soluções de equações polinomiais sobre o corpo dos números complexos. Em geral, porém, estamos interessados nas soluções de equações polinomiais com coeficientes num corpo arbitrário k, eventualmente de característica p > 0. Isso nos leva a introduzir o conceito de K/k - variedade, que analisaremos a seguir. No que se segue k é um corpo arbitrário, K/k uma extensão de corpos com K algebricamente fechado.

Indicaremos por $\mathbb{A}^n_K$ o conjunto das n-uplas de elementos de K, o n-espaço afim sobre K.

Seja J um subconjunto arbitrário do anel de polinômios $k[X_1, X_2, \ldots, X_n]$. Definimos:

$$(1) \qquad V_K(J) = \{(a_1,\ldots,a_n \in \mathbb{A}^n_K : f(a_1,\ldots,a_n) = 0 , \quad \forall f \in J\}$$

Da definição acima decorre que se A e B são subconjuntos de $k[X_1, X_2, \ldots, X_n]$ com $A \subset B$ então $V_K(A) \supset V_K(B)$. Se J é um subconjunto não vazio de $k[X_1, X_2, \ldots, X_n]$ denotamos por $\langle J \rangle$ o ideal gerado por J e por $\mathrm{Rad}(\langle J \rangle)$ o radical do ideal $\langle J \rangle$.

É fácil ver que valem as igualdades:

$$V_K(J) = V_K(\langle J \rangle) = V_K(\mathrm{Rad}(\langle J \rangle)).$$

Em vista disso passaremos a considerar somente ideais de $k[X_1, X_2, \ldots, X_n]$ em vez de subconjuntos arbitrários.

Se J_1 e J_2 são ideais de $k[X_1, X_2, \ldots, X_n]$, J_1J_2 designa o ideal gerado pelo conjunto $\{ab : a \in J_1, \ b \in J_2\}$. É claro que:

$$V_K(J_1J_2) = V_K(J_1) \cup V_K(J_2) \tag{2}$$

e se $\{J_\alpha\}$ é uma família de ideais de $k[X_1, X_2, \ldots, X_n]$ então:

$$V_K(\langle \bigcup_\alpha J_\alpha \rangle) = \bigcap_\alpha V_K(J_\alpha) \tag{3}$$

Vamos agora definir uma topologia em $\mathbb{A}^n_K$ tomando os subconjuntos $V_K(J)$ como os fechados de $\mathbb{A}^n_K$, para J percorrendo os ideais de $k[X_1, X_2, \ldots, X_n]$.

Note-se que $\mathbb{A}^n_K$ e $\emptyset$ são fechados e que, por (3), a intersecção de uma família qualquer de fechados é um fechado, e por (2), a união de dois fechados é um fechado, de modo que temos efetivamente definida uma topologia em $\mathbb{A}^n_K$, chamada a k-topologia de Zariski de $\mathbb{A}^n_K$.

DEFINIÇÃO. Uma K/k-variedade afim é um subconjunto fechado de $\mathbb{A}^n_K$ na k-topologia de Zariski.

Seja $S \subset \mathbb{A}^n_K$ um subconjunto arbitrário. Definimos o ideal de S em $k[X_1, X_2, \ldots, X_n]$ por:

$$I_k(S) = \{f \in k[X_1, X_2, \ldots, X_n] : f(P) = 0, \quad \forall P \in S\} \tag{4}$$

onde P representa uma n-upla $(a_1, \ldots, a_n) \in S$.

É claro que se $k \subset k_1 \subset K$ e $S \subset \mathbb{A}^n_K$, então:

$$I_{k_1}(S) \supset I_k(S) \tag{5}$$

$$I_{k_1}(S) \cap k[X_1, X_2, \ldots, X_n] = I_k(S) \tag{6}$$

Se S_1 e S_2 são sunconjuntos não vazios de $\mathbb{A}^n_K$ então $I_k(S_1 \cup S_2) = I_k(S_1) \cap I_k(S_2)$; se $S_1 \subset S_2$ então $I_k(S_1) \supset I_k(S_2)$. Se J é um ideal de $k[X_1, X_2, \ldots, X_n]$ e $S \subset \mathbb{A}^n_K$ temos:

$$\begin{aligned} &V_K(I_k(S)) \supset S \\ &I_k(V_K(J)) \supset J \end{aligned} \tag{7}$$

Aplicando I_k à primeira expressão de (7) obtemos $I_k(V_K(I_k(S))) \subset I_k(S)$. Como $I_k(S)$ é um ideal, a segunda expressão de (7) nos dá: $I_k(V_K(I_k(S))) \supset I_k(S)$, donde temos:

$$I_k(V_K(I_k(S))) = I_k(S) \tag{8}$$

Analogamente obtemos

$$V_K(I_k(V_K(J))) = V_K(J) \tag{9}$$

Observe-se que se $X \subset \mathbb{A}^n_K$ é um fechado na k-topologia de $\mathbb{A}^n_K$ então, por (9), $V_K(I_k(X)) = X$.

Vimos que $I_k(V_K(J)) \supset J$. Além disso, é claro que $I_k(V_K(J)) \supset \mathrm{Rad}(J)$. No caso particular em que $k = K$ temos

$I_k(V_K(J)) = Rad(J)$. Esse é o conteúdo do célebre:

NULLSTELLENSATZ (Hilbert). Seja K um corpo algebricamente fechado e J um ideal de $K[X_1, X_2, \ldots X_n]$. Se f é um polinômio de $K[X_1, X_2, \ldots, X_n]$ que se anula em todos os pontos de $V_K(J)$ então $f \in Rad(J)$.

Para uma demonstração bastante curta desse teorema ver a nota de Artin-Tate, [1], "A note on finite ring extensions". No caso em que $k \subsetneq K$ temos a versão:

PROPOSIÇÃO 1. Seja J um ideal de $k[X_1, X_2, \ldots, X_n]$, K/k uma extensão de corpos com K algebricamente fechado. Então $I_k(V_K(J)) = Rad(J)$.

PROVA. Vamos denotar por $J \otimes K$ o ideal de $K[X_1, X_2, \ldots, X_n]$ gerado por J, isto é, o ideal extendido. É claro que $V_K(J \otimes K) = V_K(J)$. Do nullstellensatz temos: $I_K(V_K(J \otimes K)) = Rad(J \otimes K)$.

Donde segue:

$$I_K(V_K(J \otimes K)) \cap k[X_1, X_2, \ldots, X_n] =$$

$$= Rad(J \otimes K) \cap k[X_1, X_2, \ldots, X_n]$$

e por (6),

$$I_k(V_K(J \otimes K)) = I_k(V_K(J)) =$$

$$= Rad(J \otimes K) \cap k[X_1, X_2, \ldots, X_n]$$

Resta provar que a contração do radical da extensão do ideal J é o próprio Rad(J). Isso é um resultado simples de álgebra comutativa que pode ser visto, por exemplo, em [2], pg 10.

OBSERVAÇÃO 1. Se K é um corpo algebricamente fechado, decorre imediatamente do nullstellensatz a existência de uma correspondência biunívoca entre os fechados de $\mathbb{A}^n_K$ e os ideais radicais (isto é, os ideais que são iguais aos seus radicais), dada por $S \to I_K(S)$ e $J \to V_K(J)$.

OBSERVAÇÃO 2. Vimos anteriormente que se X for um fechado de $\mathbb{A}^n_K$ então $V_K(I_k(X)) = X$. Se Y é um subconjunto qualquer de $\mathbb{A}^n_K$, então o seu fecho $\overline{Y}$ na k-topologia de Zariski é $V_K(I_k(Y))$ pois se V é um fechado que contém Y, então $I_k(V) \subset I_k(Y)$ e assim $V = V_K(I_K(V)) \supset V_K(I_k(Y))$, donde $V_k(I_k(Y))$ é o menor fechado que contém Y.

DEFINIÇÃO. Um espaço topológico X diz-se noetheriano se os seus subconjuntos abertos satisfazem a condição de cadeia ascendente.

DEFINIÇÃO. Um espaço topológico X é dito irredutível se satisfizer uma das três condições equivalentes:

(a) X não é a união de dois fechados prórpios de X.

(b) A intersecção de dois abertos próprios de X é não vazia.

(c) Todo aberto não vazio é denso.

Observe-se que se X é um espaço topológico irredutível e $A \subset X$ for um aberto não vazio, então A será um espaço

topológico irredutível, na topologia induzida.

Suponhamos que $V \subset \mathbb{A}^n_K$ seja uma K/k-variedade afim. É claro que a cada subconjunto fechado de V (na topologia induzida) corresponde um ideal de $k[X_1, X_2, \ldots X_n]$ que contém $I_k(V)$ pois os fechados de V na topologia induzida são os fechados de $\mathbb{A}^n_K$ contidos em V. Reciprocamente, a cada ideal de $k[X_1, X_2, \ldots, X_n]$ que contém $I_k(V)$ corresponde um subconjunto fechado de V.

É bem conhecido que os ideais de $k[X_1, X_2, \ldots, X_n]$ que contém $I_k(V)$ estão em correspondência bijetora com os ideais de $k[X_1, X_2, \ldots, X_n]/I_k(V)$. No que se segue denotaremos esse quociente por k[V]. Esse anel é chamado de anel de coordenadas afins ou anel das funções polinomiais em V. Como $k[X_1, \ldots, X_n]$ é um anel noetheriano, então k[V] será noetheriano, e portanto toda cadeia ascendente de ideais de $k[X_1, \ldots, X_n]$ que contém $I_k(V)$ estaciona, ou seja, toda cadeia descendente de fechados de V é estacionária, e portanto V é um espaço topológico noetheriano com a k-topologia de Zariski induzida.

PROPOSIÇÃO 2. A K/k-variedade afim V com a k-topologia induzida é um espaço topológico irredutível se e só se $I_k(V)$ for um ideal primo.

PROVA. Suponhamos que V seja irredutível e que f_1, f_2 sejam dois polinômios fora de $I_k(V)$. Seja W_i o conjunto dos pontos de V onde f_i se anula, i = 1, 2. Então W_i é uma K/k-variedade de $\mathbb{A}^n_K$ e também um fechado próprio de V. Como V é irredutível, $W_1 \cup W_2 \subsetneq V$. Seja x um ponto de $V-(W_1 \cup W_2)$. Então $f_i(x) \neq 0$, i = 1, 2, e portanto $f_1 \cdot f_2 \notin I_k(V)$, donde $I_k(V)$ é um ideal primo. Reciprocamente, se $I_k(V)$ for um ideal primo, seja $V = V_1 \cup V_2$, onde V_i é um fechado de V, i = 1, 2.

Suponhamos que $V_2 \neq V$. Provaremos que $V_1 = V$ e que, portanto, V é irredutível. Temos:

$$I_k(V) = I_k(V_1 \cup V_2) = I_k(V_1) \cap I_k(V_2) \supset I_k(V_1) \cdot I_k(V_2)$$

como $I_k(V)$ é primo e $I_k(V_2) \not\supseteq I_k(V)$ segue que $I_k(V) \supset I_k(V_1)$, ou seja $V = V_1$. C.Q.D.

PROPOSIÇÃO 3. Num espaço topológico noetheriano X todo fechado não vazio F pode ser expresso como a união finita $F = F_1 \cup \ldots \cup F_n$ de fechados irredutíveis de X. Se eliminarmos as redundâncias, isto é, se $F_i \not\supset F_j$ para $i \neq j$, então a decomposição é única.

PROVA. Seja $\mathbb{F}$ o conjunto dos fechados não vazios de X que não podem ser expressos como uma reunião finita de fechados irredutíveis. Suponhamos que $\mathbb{F}$ seja não vazio. Como X é noetheriano F possui um elemento minimal Y. Logo Y não pode ser irredutível e portanto $Y = Y_1 \cup Y_2$ onde Y_i é um fechado próprio de Y, $i = 1, 2$. Pela minimalidade de Y, $Y_i \notin \mathbb{F}$, donde temos uma contradição, e portanto $\mathbb{F} = \emptyset$.

Se $F = F_1 \cup F_2 \cup \ldots \cup F_n$, com F_i fechado e irredutível e se $F = Y_1 \cup \ldots \cup Y_m$ com Y_i fechado e irredutível, $Y_i \not\subset Y_j$ se $i \neq j$, como $Y_1 \subset F_1 \cup \ldots \cup F_n = F$, $Y_1 = \bigcup_{i=1}^{n} (F_i \cap Y_1)$ e como Y_1 é irredutível, $Y_1 \subset F_{i(1)}$. Repetindo o argumento para $F_{i(1)}$, temos $F_{i(1)} \subset Y_j$ para algum índice j. Como por hipótese $Y_i \not\subset Y_j$ se $i \neq j$, segue que $j = 1$, ou seja, $Y = F_{i(1)}$, donde $m \leq n$. Invertendo o argumento resulta $n \leq m$. C.Q.D.

COROLÁRIO 1. Toda K/k-variedade afim V pode ser escrita como uma reunião finita de K/k-variedades afins irredutíveis V_i, com $V_i \not\supset V_j$ se $i \neq j$.

DEFINIÇÃO. Se X é um espaço topológico, definimos a dimensão de X (denotada dimX) como o supremo de todos os inteiros n tais que existe uma cadeia $F_0 \subset F_1 \subset \ldots \subset F_n$ de fechados irredutíveis e distintos de X. Definimos a dimensão de uma K/k-variedade afim como a sua dimensão como espaço topológico.

OBSERVAÇÃO. Em vista do corolário 1, $\dim V = \max_i \dim V_i$ onde as V_i são as componentes irredutíveis de V.

DEFINIÇÃO. Num anel A, a altura de um ideal primo P é o supremo de todos os inteiros n para os quais existe uma cadeia $P_0 \subset P_1 \subset \ldots \subset P_n = P$ de ideais primos distintos. Define-se a dimensão de Krull de A, denotada dimA, como o supremo das alturas de todos os ideais primos de A.

PROPOSIÇÃO 4. Se Y é uma K/k-variedade afim então a dimensão de Y é igual à dimensão de Krull de k[Y].

PROVA. Já vimos que os fechados irredutíveis de Y correspondem a ideais primos de $k[X_1, X_2, \ldots X_n]$ que contém $I_k(Y)$. Estes por sua vez correspondem a ideais primos de k[Y] e reciprocamente. Assim a dimensão de Y é o comprimento da mais longa cadeia de ideais primos em k[Y], que é sua dimensão de Krull. C.Q.D.

Se Y é uma K/k-variedade afim irredutível a proposição 2 garante que o anel de coordenadas afins k[Y] é um domínio. O corpo de frações de k[Y], denotado k(Y), é chamado o corpo das funções racionais em Y. Como k[Y] é um domínio finitamente gerado como k-álgebra, um resultado de álgebra comutativa nos garante que a dimensão de Krull de k[Y] (e portanto a dimensão de Y) é igual ao grau de transcendência da extensão k(Y)/k (Matsumura, Commutative Algebra, cap 5, § 14).

DEFINIÇÃO. Uma K/k-variedade afim irredutível de dimensão 1 é chamada curva afim.

Seja V uma K/k variedade afim irredutível e f uma função racional em V (isto é, $f \in k(V)$). Se P é um ponto de V, dizemos que f está definida em P se para certos h, $g \in k[V]$, $f = h/g$ e $g(P) \neq 0$. Definimos $O_P(V)$ como o conjunto das funções racionais em V que estão definidas em P. É imediato verificar que $O_P(V)$ é isomarfo ao localizado de k[V] em relação ao ideal das funções polinomiais de k[V] que se anulam em P. Assim $O_P(V)$ é um subanel de k(V) que contém k[V]. O seu único ideal maximal é $M_P = \{f \in O_P(V) : f(P) = 0\}$. Em particular se k = K for algebricamente fechado, $O_P(V)/M_P \simeq K$.

§2 - Variedades projetivas

De modo análogo ao caso afim, começamos por definir o n-espaço projetivo sobre um corpo arbitrário k como o conjunto das (n+1)-uplas $(a_0, a_1, \ldots, a_n)$ de elementos não todos nulos de k sob a relação de equivalência dada por $(a_0, a_1, \ldots, a_n) \sim (\lambda a_0, \lambda a_1, \ldots, \lambda a_n)$ para todo $\lambda \in k$, $\lambda \neq 0$. Denotaremos por $\mathbb{P}^n_k$ o n-espaço projetivo sobre k. Um elemento de $\mathbb{P}^n_k$ é chamado ponto. Se P é um ponto, uma (n+1)-upla $(a_0, a_1, \ldots, a_n)$ na classe de equivalência P é chamada um conjunto de coordenadas homogêneas para P. Observe-se que embora não possamos falar na i-ésima coordenada de P, a_i, podemos falar que $a_i = 0$ ou que $a_i \neq 0$, e assim definimos o conjunto $U_i = \{(x_0, x_1, \ldots, x_n) \in \mathbb{P}^n_k : x_i \neq 0\}$. Se $P \in U_i$, $P = (x_0, x_1, \ldots, x_n)$, podemos associar à P a n-upla $(x_0/x_i, x_1/x_i, \ldots, x_n/x_i)$ com x_i/x_i omitido. Note-se que o quociente x_j/x_i independe da particular representação de P. Temos então uma aplicação $\phi_i : U_i \to \mathbf{A}^n_k$ que estabelece uma correspondência bijetora entre os pontos de U_i e os pon

tos de $\mathbb{A}^n_k$. Além disso $\mathbb{P}^n_k = \bigcup_{i=1}^{n} U_i$.

Se $f \in k[X_0, X_1, \ldots, X_n]$ é um polinômio, não podemos utilizá-lo para definir uma função em $\mathbb{P}^n_k$, pela não unicidade das coordenadas homogêneas. Entretanto, se f for um polinômio homogêneo de grau d, isto é, se $f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n)$, podemos dizer que se f tem um zero ou não na classe de $(a_0, a_1, \ldots, a_n)$. Se J é um conjunto de polinômios homogêneos de $k[X_0, X_1, \ldots, X_n]$ e K/k uma extensão de corpos, definimos:

$$V_K(J) = \{P \in \mathbb{P}^n_k : f(P) = 0 \quad \forall f \in J\}$$

Dizemos que um ideal de $k[X_0, X_1, \ldots, X_n]$ é homogêneo se for gerado por elementos homogêneos. Como no caso afim, se J é como acima, vale $V_K(J) = V_K(\langle J \rangle)$ e portanto passaremos a considerar somente ideais homogêneos de $k[X_0, \ldots, X_n]$.

Definimos a k-topologia de Zariski de $\mathbb{P}^n_K$ de modo análogo ao caso afim, tomando os subconjuntos $V_K(J)$ como os fechados, onde J percorre o conjunto dos ideais homogêneos de $k[X_0, X_1, \ldots X_n]$. A verificação de que de fato temos uma topologia é análoga ao caso afim. Obtida a topologia, as noções de subconjunto irredutível e de dimensão se aplicam naturalmente.

DEFINIÇÃO. Uma K/k-variedade projetiva é um subconjunto fechado de $\mathbb{P}^n_K$, com a topologia induzida. A dimensão de uma variedade projetiva é a sua dimensão como espaço topológico.

Se S é um subconjunto não vazio de $\mathbb{P}^n_K$, definimos $I_k(S)$ como o ideal gerado pelo conjunto $\{f \in k[X_0, X_1, \ldots, X_n]$,

homogêneo, : $f(P) = 0$, $\forall P \in S\}$, e portanto é um ideal homogêneo. Se I é um ideal homogêneo, I é um ideal primo se e só se para dois quaisquer polinômios homogêneos f e g, se $f.g \in I$ então ou $f \in I$ ou $g \in I$. Com esse resultado, podemos repetir quase inteiramente a prova dada no caso afim e concluir que V é uma K/k-variedade projetiva irredutível se e só se $I_k(V)$ for um ideal primo. Assim o anel $k_h[V] = k[X_0, X_1, \ldots, X_n]/I_k(V)$ é um domínio e é chamado anel de coordenadas homogêneas de V. O corpo de frações de $k_h[V]$, denotado $k_h(V)$, é chamado o corpo de funções homogêneas de V.

Ao contrário do caso afim, os elementos de $k_h(V)$ em geral não determinam funções em V. No que se segue veremos como construir de fato um corpo de funções em V.

PROPOSIÇÃO 1. Seja $I \subset k[X_0, X_1, \ldots, X_n]$ um ideal homogêneo. Se $F = \sum_{i=0}^{m} F_i$ é um elemento de I, onde F_i é um polinômio homogêneo de grau i, então tem-se que $F_i \in I$, $i = 0,1,\ldots,m$.

PROVA. Basta provar que $F_m \in I$, pois então $F - F_m \in I$ e o resto segue por indução. Sejam $\{f^{(\alpha)}\}$ os geradores homogêneos de I e seja d_α o grau de $f^{(\alpha)}$.

Pondo $F = \sum A^{(\alpha)} f^{(\alpha)}$ e decompondo cada $A^{(\alpha)}$, $A^{(\alpha)} = \sum_{j=0}^{b_\alpha} A_j^{(\alpha)}$, onde $A_j^{(\alpha)}$ é homogêneo de grau j temos: $F_m = \sum A_{m-d_\alpha}^{(\alpha)} f^{(\alpha)}$, donde $F_m \in I$. C.Q.D.

Um elemento $\overline{g}$ de $k_h[V]$ é dito homogêneo de grau d se existir um polinômio homogêneo g de grau d em $k[X_0, X_1, \ldots, X_n]$ tal que $\overline{g} = g + I_k(V)$.

Se $\overline{f}$ e $\overline{g}$ são elementos de $k_h[V]$ homogêneos e de mesmo grau d, então $\overline{f}/\overline{g}$ efetivamente define uma função em V (se $g \not\equiv 0$) pois

$$\frac{f(\lambda x)}{g(\lambda x)} = \frac{\lambda^d f(x)}{\lambda^d g(x)} = \frac{f(x)}{g(x)}$$

de modo que $f(x)/g(x)$ independe da escolha de coordenadas homogêneas, e claramente independe da escolha dos representantes f e g das classes $\overline{f}$ e $\overline{g}$.

O corpo de funções de V, denotado k(V), é definido como o subconjunto de $k_h(V)$ que consiste das funções ϕ para as quais existem $f, g \in k_h[V]$ elementos homogêneos de mesmo grau, tais que $\phi = \overline{f}/\overline{g}$. Os elementos de k(V) são chamados de funções racionais em V.

Seja $P \in V$, $z \in k(V)$. Dizemos que z está definida em P se $z = \overline{f}/\overline{g}$ para certos $\overline{f}$, $\overline{g}$ homogêneos de mesmo grau e $g(P) \neq 0$. Seja $O_p(V)$ o subconjunto de k(V) que consiste das funções que estão definidas em P. Então $O_p(V)$ é um subanel de k(V) e é um anel local cujo único ideal maximal é $M_p = \{z : z = \overline{f}/\overline{g} \ , \ g(P) \neq 0 \ , \ f(P) = 0\}$.

Seja V uma K/k-variedade afim, e I o seu ideal em $k[X_1, \ldots, X_n]$ (o caso projeto é inteiramente análogo). Seja $\overline{I} = I \otimes K \subset K[X_1, \ldots, X_n]$ o ideal gerado por I. Definimos $\overline{V} = V_K(\overline{I})$ como a variedade correspondente a V obtida por extensão de escalares. Conjuntisticamente, $V = \overline{V}$.

No que se segue vamos explorar um pouco as relações entre variedades afins e variedades projetivas. Por simplicidade vamos supor que $k = K$ é um corpo algebricamente fechado. Os n-espaços afim e projetivo sobre K serão denotados respectivamente $\mathbf{A}^n$ a $\mathbf{P}^n$.

Se F é um polinômio homogêneo de $K[X_0, X_1, \ldots, X_n]$, definimos $F_* \in K[X_1, \ldots, X_n]$ pondo $F_* = F(1, X_1, X_2, \ldots, X_n)$. Reciprocamente para qualquer polinômio $f \in K[X_1, X_2, \ldots, X_n]$ de grau d, pomos $f = f_0 + f_1 + \ldots + f_d$ onde f_i é um polinômio homogêneo de grau i, e definimos $f^* \in K[X_0, X_1, \ldots, X_n]$ como

$$f^* = X_0^d f_0 + X_0^{d-1} f_1 + \ldots + f_d = X_0^d f(X_1/X_0, \ldots, X_n/X_0)$$

e f^* é um polinômio homogêneo de grau d.

Esses processos podem ser entendidos como uma desomogenização e homogenização de polinômios em relação à variável X_0. É imediata a

PROPOSIÇÃO 2. Se F, G são polinômios homogêneos de $K[X_0, X_1, \ldots, X_n]$ e f, g polinômios arbitrários de $K[X_1, \ldots, X_n]$ então:

(a) $(FG)_* = F_* G_* \quad ; \quad (fg)^* = f^* g^*$

(b) Se r é a maior potência de X_0 que divide F, então $X_0^r (F_*)^* = F$ e $(f^*)_* = f$

(c) $(F+G)_* = F_* + G_* \quad ; \quad X_0^t (f+g)^* = X_0^r f^* + X_0^s g^*$
onde $t = r + s - \text{grau}(f+g)$,
$r = \text{grau}(g)$,
$s = \text{grau}(f)$.

Definimos anteriormente os subconjuntos U_i de $\mathbf{P}^n$ como $U_i = \{(x_0, x_1, \ldots, x_n) \in \mathbf{P}^n : x_i \neq 0\}$. É claro que cada $P \in U_i$ possui um único conjunto de coordenadas homogêneas da forma: $P = (X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$. As coordena

das $(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$ são chamadas coordenadas não-homogêneas para P em relação à U_i. Definindo $\psi_i : \mathbf{A}^n \to U_i$ por $\psi_i(X_1, X_2, \ldots, X_n) = (X_1, X_2, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n)$, $\psi_i = \phi_i^{-1}$, onde ϕ_i é a aplicação já definida no início do §2, podemos considerar $\mathbf{A}^n$ como subconjunto de $\mathbf{P}^n$. Pomos $H_\infty = \mathbf{P}^n - U_0 = \{(X_0, \ldots, X_n) : X_0 = 0\}$ e é usual dizer que H_∞ é o hiperplano no infinito.

A correspondência $(0, X_1, \ldots, X_n) \leftrightarrow (X_1, \ldots, X_n)$ mostra que H_∞ pode ser identificado com $\mathbf{P}^{n-1}$.

Seja V uma variedade afim em $\mathbf{A}^n$, $I = I_K(V)$ o seu ideal em $K[X_1, X_2, \ldots, X_n]$. Seja I^* o ideal em $K[X_0, X_1, \ldots, X_n]$ gerado pelos f^*, $f \in I$. Então I^* é um ideal homogêneo, e definimos V^* com $V_K(I^*)$. Reciprocamente, seja V uma variedade projetiva em $\mathbf{P}^n$, $I = I_K(V)$ o seu ideal homogêneo. Analogamente seja I_* o ideal em $K[X_1, X_2, \ldots, X_n]$ gerado pelos f_*, $f \in I$. Definimos V_* como $V_K(I_*) \subset \mathbf{A}^n$.

PROPOSIÇÃO 3. Nas condições acima valem:

(a) Se $V \subset \mathbf{A}^n$, $\psi_0(V) = V^* \cap U_0$ e $(V^*)_* = V$

(b) Se $V \subset W \subset \mathbf{A}^n$, então $V^* \subset W^* \subset \mathbf{P}^n$

Se $V \subset W \subset \mathbf{P}^n$, então $V_* \subset W_* \subset \mathbf{A}^n$

(c) Se V é irredutível em $\mathbf{A}^n$, então V^* será irredutível em $\mathbf{P}^n$.

(d) Se $V = \bigcup_i V_i$ é a decomposição de V em suas componentes irredutíveis, em $\mathbf{A}^n$, então $V^* = \bigcup_i V_i^*$ é a decomposição de V^* em suas componentes irredutíveis, em $\mathbf{P}^n$.

(e) Se $V \subset \mathbb{A}^n$, então V^* é o menor fechado de $\mathbb{P}^n$ que contém $\psi_0(V)$.

PROVA. Se $(x_1, x_2, \ldots, x_n) \in V$, sua imagem por ψ_0 será $(1, x_1, \ldots, x_n) \in U_0$. Vamos mostrar que $(1, x_1, \ldots, x_n)$ está em $V^* = V_K(I^*)$. Para tanto é suficiente verificar que se $f \in I$, então $f^*(1, x_1, \ldots, x_n) = 0$, o que é claro. A recíproca é análoga, o que prova que $\psi_0(V) = V^* \cap U_0$. O item (b) da proposição 2 prova que $(V^*)_* = V$. Isso prova (a). A parte (b) é óbvia.

Para provar (e), suponhamos que W seja um fechado de $\mathbb{P}^n$ que contém $\psi_0(V)$. Se $F \in I(W)$ então $F_* \in I(V)$, donde $F = X_0^r (F_*)^* \in I(V)^*$ donde $I(W) \subset I(V)^*$, e portanto $W \supset V^*$, o que prova (e). Para provar (c), note-se que se $V \subset \mathbb{A}^n$, $I = I(V)$, então um polinômio homogêneo F pertencerá a I^* se e só se $F_* \in I$. Se I for primo, então é claro que I^* será primo, o que prova (c).

Para provar (d), por (e), se V_i é irredutível, V_i^* será irredutível e por (a), (b), se $V_i \not\subset V_j$ então $V_i^* \not\subset V_j^*$, e isso prova (d). C.Q.D.

Se V é um fechado de $\mathbb{A}^n$, $V^* \subset \mathbb{P}^n$ é chamado o fecho projetivo de V. Se $f \in K_h[V^*]$ é um elemento homogêneo de grau d, podemos definir $f_* \in K[V]$ assim: tomamos um polinômio homogêneo de grau d, $F \in K[X_0, X_1, \ldots, X_n]$ tal que $f = F + I_K(V^*)$ e tomamos $f_* = F_* + I_K(V)$. É claro que a definição independe da particular escolha de F.

Definimos assim um isomarfismo natural $\alpha : K(V^*) \to K(V)$ dado por $\alpha(f/g) = f_*/g_*$. α está bem definido e é um marfismo de corpos e α é sobrejetor pois se $l/h \in K(V)$, grau(l) = m, grau(h) = n, então l^*, $h^* \in K[V^*]$ e $\frac{X_0^{n-m} l^*}{h^*} \in K(V^*)$ e sua imagem é precisamente l/h.

Se $P \in V$, então α induz um isomorfismo entre $O_P(V^*)$ e $O_P(V)$ (estamos aqui pensando em R como um ponto de V^* via ψ_0).

Até agora definimos variedades afins e projetivas e examinamos um pouco as relações entre elas. Porém ainda não definimos transformações entre duas variedades quaisquer. No que se segue continuaremos no mesmo contexto que antes, isto é, k = K é um corpo algebricamente fechado.

DEFINIÇÃO. Seja V uma variedade afim de $\mathbb{A}^n$. Uma função $f:V \to K$ é regular no ponto $P \in V$ se existir uma vizinhança aberta U com $P \in U \subseteq V$ e polinômios $g, h \in K[X_1,\ldots,X_n]$ tal que h não se anula em nenhum ponto de U e $f = g/h$ em U. Dizemos que f é regular em V se for regular em todo ponto de V.

DEFINIÇÃO: Seja V uma variedade projetiva em $\mathbb{P}^n$. Uma função $f:V \to K$ é regular no ponto $P \in V$ se existir uma vizinhança aberta U com $P \in U \subseteq V$, e polinômios homogêneos de mesmo grau, $g, h \in K[X_0,X_1,\ldots,X_n]$ tais que h não se anula em U e $f = g/h$ em U. Dizemos que f é regular em V se for regular em todos os pontos de V.

Como ficou claro até aqui, somente temos interesse em variedades afins ou projetivas que sejam irredutíveis. De modo que, para tudo o que seguirá neste e nos demais capítulos, estamos supondo que, salvo menção contrária, toda variedade afim ou projetiva é irredutível.

DEFINIÇÃO: Sejam X e Y duas variedades sobre K. (Podem ser ambas afins, projetivas ou uma afim e outra projetiva). Um morfismo $\phi: X \to Y$ é uma aplicação contínua tal que para todo aberto $V \subseteq Y$ e para toda função regular $f:V \to K$, a função $f \circ \phi \mid \phi^{-1}(V) \to K$ é regular.

Temos em particular a noção de isomorfismo de variedades $\phi: X \to Y$, como um morfismo que admite um mofirsmo inverso $\psi: Y \to X$ com $\psi \circ \phi = id_X$ e $\phi \circ \psi = id_Y$.

Em vista da definição acima, é fácil ver que $\mathbb{A}^n$ e U_0 são isomorfos como variedades.

§3 - Curvas não Singulares

Já vimos que se V é uma variedade, k(V)/k é uma extensão finitamente gerada e a dimensão de V é igual ao grau de transcendência de k(V)/k. Seja K um corpo algebricamente fechado, $K \supset k$. Uma K/k-variedade (afim ou projetiva) de dimensão 1 foi chamada curva (afim ou projetiva). Se V é uma curva sobre k, o seu corpo de funções $\mathbb{K} = k(V)$ é um corpo de funções algébricas de uma variável sobre k pois, como V é curva, a extensão k(V)/k tem grau de transcendência 1 isto é, existe um elemento $x \in k(V)$ transcendente sobre k tal que k(V)/k(x) é algébrica. Como k(V)/k é finitamente gerada, k(V)/k(x) será portanto finita.

No que se segue, suporemos que k=K seja um corpo algebricamente fechado, e em lugar de $\mathbb{A}^n_k$ e $\mathbb{P}^n_k$ escreveremos somente $\mathbb{A}^n$ e $\mathbb{P}^n$.

PROPOSIÇÃO 1. Seja $V \subset \mathbb{A}^n$ uma variedade afim sobre k e V^* o seu fecho projetivo em $\mathbb{P}^n$.

(a) $\dim V^* = \dim V$

(b) $\dim V = 0$ se e só se V for um ponto.

(c) toda subvariedade própria de uma cruva afim é um ponto.

PROVA. (a) decorre do fato de que V e V^* possuem corpos de funções isomorfos. Para provar (b), suponhamos que dim V = 0. Então k(V)/k é uma extensão algébrica, e como k é algebricamente fechado, k(V) = k, donde k[V] = k, o que acarreta $I_k(V)$ maximal, e assim V = {P} . A recíproca é clara.

Para provar (c), seja W uma subvariedade própria de V, e seja R = k[V] , P o ideal primo de R correspondente a W. (isto é P é o kernel do epimorfismo natural η: k[V] → k[W])

(c) estará provado se mostrarmos que R/P ≃ k.

Consideremos a aplicação natural de k em R/P. Provaremos que ela é sobrejetora.

Suponhamos que existe x ∈ R tal que x+P não seja imagem de nenhum elemento de k.

Como W é própria, P ≠ 0, e portanto existe y ∈ P, y ≠ 0. Como o grau de transcendência de k(V) sobre k é 1, y satisfaz um polinômio irredutível com coeficientes em k(x), $F(x,y) = \sum_i a_i(x)y^i = 0$. Então decorre que $a_0(x) \neq 0$ e portanto $a_0(x) \in P$. Donde x + P ∈ R/P satisfaz o polinômio $a_0 \in k[x]$.

Mas como k é algebricamente fechado, x + P ∈ k, ou seja, a aplicação dada é sobrejetora. C.Q.D.

Estamos nos preparando para provar o resultado mais importante deste capítulo, o teorema 2.

Vamos agora relembrar o contexto em que estamos: k é um corpo algebricamente fechado, e se V é uma variedade afim ou projetiva sobre k, V é sempre irredutível.

DEFINIÇÃO. Seja **C** uma cruva arbitrária e P ∈ **C**. Dizemos que P é não singular se $O_P(\mathbf{C})$ for um anel de valorização discreta. A curva **C** é dita não singular se todos os seus pontos forem não singulares.

Em geral, se $Y \subseteq \mathbf{A}^n$ é uma variedade afim e $f_1,\ldots,f_m \in k[X_1,X_2,\ldots,X_n]$ é um conjunto de geradores de $I_k(Y)$, diz-se que Y é não singular no ponto P ∈ Y se o posto da matriz $||(\partial f_i/\partial X_j)(P)||$ é n-r onde r = dim Y. Y é dita não singular se for não singular em todos os seus pontos.

Essa definição é boa (pode-se mostrar que ela independe do particular conjunto de geradores escolhido), porém tem a desvantagem de depender (aparentemente) da imersão de Y num espaço afim. Entretanto, prova-se ([5] , pg.32) que Y é não singular em P ∈ Y se e só se o anel local $O_P(Y)$ é um anel local regular, ou seja, se dim $O_P(Y) = \dim_k M_P/M_P^2$. Em particular, se Y for uma curva afim, prova-se que $O_P(Y)$ é um anel local regular se e só se for um anel de valorização discreta ([2] , pg.94). Sendo então um conceito intrínseco, extendemos a definição de não-singularidade para variedades projetivas, via a regularidade do anel local $O_P(Y)$. Como estamos interessados em curvas, a definição dada acima é a mais adequada aos nossos propósitos.

OBSERVAÇÃO. A aplicação $(x_1,\ldots,x_n) \longmapsto (0,x_1,\ldots,x_n)$ dá um isomorfismo de variedades entre $\mathbf{P}^{n-1}$ e $H_0 = \mathbf{P}^n - U_0 \subset \mathbf{P}^n$. Se uma variedade V em $\mathbf{P}^n$ estiver contida em H_0, V é isoforma a uma variedade de $\mathbf{P}^{n-1}$.

Assim, dada uma variedade projetiva, existe um n de modo que ela é isomorfa a uma subvariedade V de $\mathbf{P}^n$ que não está contida em nenhum hiperplano.

TEOREMA 1. Seja **C** uma curva projetiva definida sobre k. Se

ja L um corpo arbitrário contendo $k(\mathbf{C})$ e A um anel de valorização discreta de L que contém k ($A \supset k$), com ideal maximal M. Suponhamos que $A \not\supset k(\mathbf{C})$. Então existe um ponto $P \in \mathbf{C}$ tal que $A \supset O_P(\mathbf{C})$ e $M \supset M_P$, onde M_P é o ideal maximal de O_P.

PROVA. Em vista da observação anterior podemos supor que $\mathbf{C}$ seja uma variedade em $\mathbb{P}^n$ com $\mathbf{C} \cap U_i \neq 0$, $i = 0, 1, \ldots, n$. Então em $k_h[\mathbf{C}] = k[X_0, X_1, \ldots, X_n]/I_k(\mathbf{C}) = k[x_0, x_1, \ldots, x_n]$ $x_i = X_i + I_k(\mathbf{C})$, cada $x_i \neq 0$. Observe que $x_i/x_j \in k(\mathbf{C})$. Seja $N = \max_{i,j}\{v(x_i/x_j)\}$, onde v é a valorização associada do anel A. Fazendo uma mudança de coordenadas se necessário, podemos supor que $N = v(x_j/x_0)$ para certo j. Então para todo $i, v(x_i/x_0) = v((x_j/x_0)\cdot(x_i/x_j)) = N - v(x_j/x_i) \geq 0$.

Seja $\mathbf{C}_*$ a curva afim correspondente à $\mathbf{C} \cap U_0$.

Seja $\theta: k[X_1, \ldots, X_n] \to k[x_1/x_0, \ldots, x_n/x_0]$ a aplicação natural que leva $X_i \to x_i/x_0$. É claro que θ é um epimorfismo de anéis. Se $f \in \mathrm{Ker}\theta$, $f(x_1/x_0, \ldots, x_n/x_0) \in I_k(\mathbf{C})$, donde, se $r = \mathrm{grau}(f)$, $x_0^r f(x_1/x_0, \ldots, x_n/x_0) \in I_k(\mathbf{C})$, donde $f^* \in I_k(\mathbf{C})$, donde $(f^*)_* \in I_k(\mathbf{C})_* \subset I_k(\mathbf{C}_*)$. Mas pela proposição 2, (b), segue que $f \in I_k(\mathbf{C}_*)$. Ou seja, $\mathrm{Ker}\theta \subset I_k(\mathbf{C}_*)$. Mas claramente $I_k(\mathbf{C}_*) \subset \mathrm{Ker}\theta$, donde provamos que

$$k[\mathbf{C}_*] \simeq k[x_1/x_0, \ldots, x_n/x_0].$$

Como $v(x_i/x_0) \geq 0$, e $A \supset k$, segue das considerações acima que $A \supset k[\mathbf{C}_*]$. Seja $J = M \cap k[\mathbf{C}_*]$. Então J é um ideal primo e portanto corresponde a uma subvariedade $W \subseteq \mathbf{C}_*$.

Se $W = \mathbf{C}_*$, então $J = (0)$ e portanto todo elemento não nulo de $k[\mathbf{C}_*]$ é inversível em A. Nesse caso teríamos $k(\mathbf{C}_*) \subset A$, ou seja, $k(\mathbf{C}) \subset A$, contra a hipótese. Logo, pela

proposição 1, (b), §3, W = {P} e se $f/g \in O_P(\mathbf{C}_*) = O_P(\mathbf{C})$, $f, g \in k[C_*]$, $g \notin J$, assim $v(f/g) = v(f) - v(g)$, mas como $g \notin M$, $v(g) = 0$, donde $v(f/g) \geq 0$, donde $A \supset O_P(\mathbf{C}_*) = O_P(C)$ e claramente $M \supset M_P$. C.Q.D.

COROLÁRIO 1. Seja $\mathbf{C}$ uma curva projetiva não singular definida sobre k. Então existe uma correspondência bijetora entre os pontos de $\mathbf{C}$ e os anéis de valorização discreta de $k(\mathbf{C})$ que contém k. Se $P \in \mathbf{C}$, o correspondente anel de valorização discreta é $O_P(\mathbf{C})$.

PROVA. Como a curva $\mathbf{C}$ é não singular, $O_P(\mathbf{C})$ é um anel de valorização discreta. Suponhamos que $O_P(\mathbf{C}) = O_Q(\mathbf{C})$ para certos pontos P, $Q \in \mathbf{C}$. Como sempre existe um hiperplano $H \subset \mathbb{P}^n$ tal que P, $Q \notin H$, posso considerar que $\mathbf{C}$ é afim, e nesse caso $O_P(\mathbf{C}) = \{f/g : f, g \in k[\mathbf{C}]; g(P) \neq 0\} = k[\mathbf{C}]_M$, onde $k[\mathbf{C}]_M$ indica o localizado de $k[\mathbf{C}]$ em relação ao ideal maximal $M = \{f \in k[\mathbf{C}] : f(P) = 0\}$. Analogamente $O_Q(\mathbf{C}) = k[C]_N$, onde N é o ideal maximal $N = \{g \in k[\mathbf{C}] : g(Q) = 0\}$. Assim, se $k[\mathbf{C}]_M = k[\mathbf{C}]_N$, temos: se $g \notin M$ então $g \notin N$ e vice versa, ou seja, M = N. Os ideais M e N de k[C]correspondem a ideais maximais $\overline{M}$ e $\overline{N}$ de $k[X_1, X_2, \ldots, X_n]$, $\overline{N} = I_k(\{Q\})$ e $\overline{M} = \{f \in k[X_1, X_2, \ldots, X_n] : f(P) = 0\} = I_k(\{P\})$. Mas então $\overline{M} = \overline{N}$, e, em geral vale: se V e W são fechados de $\mathbf{A}^n_k$, então V = W se e só se $I_k(V) = I_k(W)$. (lembrando que k é algrbricamente fechado). Donde segue, por esse resultado que P = Q. Agora, se A é um anel de valorização discreta de k(C) que contém k, pelo teorema 1 existe $P \in \mathbf{C}$ tal que $A \supset O_P(\mathbf{C})$. Mas pela maximalidade dos anéis de valorização discreta (lema 3, §2, Cap. I) segue que $A = O_P(\mathbf{C})$. C.Q.D.

Tendo provado esse corolário, vamos agora considerar o caso em que $\mathbf{C}$ é uma curva projetiva definida sobre um

corpo finito $\mathbf{F}_q$. Diremos $\mathbf{C}/\mathbf{F}_q$ é não singular se a curva obtida pela extensão de escalares à $\overline{\mathbf{F}}_q$ o for.

Já vimos que $\overline{\mathbf{F}}_q/\mathbf{F}_q$ é uma extensão de Galois. Seja $G = \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$. Se J é um ideal homogêneo de $\mathbf{F}_q[X_o, X_1, \ldots, X_n]$, consideremos a variedade $Y = V_{\overline{\mathbf{F}}_q}(J) \subset \mathbf{P}^n_{\overline{\mathbf{F}}_q}$. Então o grupo de Galois G age naturalmente em Y, e cada uma das órbitas é finita, pelo comentário que se segue à proposição 6 do §1 do Capítulo I. Uma órbita da ação de G em Y é chamada de ponto fechado de Y.

TEOREMA 2. Seja C uma curva projetiva não singular definida sobre um corpo finito $\mathbf{F}_q$. (Isto é, $\mathbf{C}$ é uma $\overline{\mathbf{F}}_q/\mathbf{F}_q$- variedade projetiva de dimensão 1). Então existe uma correspondência bijetora entre os pontos fechados de $\mathbf{C}$ e os anéis de valorização discreta de $\mathbf{F}_q(\mathbf{C})$ que contém $\mathbf{F}_q$, que a cada ponto fechado p de $\mathbf{C}$ associa o anel $O_p(C)$, onde $P \in p$.

PROVA. Seja I o ideal homogêneo de $\mathbf{C}$ e $\overline{I} = I \otimes \overline{\mathbf{F}}_q \subset \overline{\mathbf{F}}_q[X_o, X_1, \ldots, X_n]$ a extensão de I (vide pag 28). Pondo $\overline{\mathbf{C}} = V_{\overline{\mathbf{F}}_q}(\overline{I})$, temos que, como conjuntos , $C = \overline{C}$. Se $P \in \mathbf{C} = \overline{\mathbf{C}}$, por definição $O_P(\overline{C})$ é um anel de valorização discreta de $\overline{\mathbf{F}}_q(\overline{\mathbf{C}})$. Seja $\overline{V} = \overline{V}(\overline{\mathbf{F}}_q(\overline{C})/\overline{\mathbf{F}}_q)$ o conjunto dos anéis de valorização discreta de $\overline{\mathbf{F}}_q(\overline{\mathbf{C}})$ que contém $\overline{\mathbf{F}}_q$ e $V = V(\mathbf{F}_q(\mathbf{C})/\mathbf{F}_q)$ o conjunto dos anéis de valorização discreta de $\mathbf{F}_q(\mathbf{C})$ que contém $\mathbf{F}_q$. Consideremos a ação de $G = \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ em $\overline{V}$ definida assim: se $\sigma \in G$, $O_P(\overline{C}) \in \overline{V}$, $\sigma \cdot O_P(\overline{C}) = O_{\sigma(P)}(\overline{C})$.

Seja $R:\overline{V} \to V$ a aplicação natural dada por $R(O_P(\overline{C})) = O_P(\overline{C}) \cap \mathbf{F}_q(C)$. Se pensarmos em $\overline{V}$ como o conjunto das valorizações discretas de $\overline{\mathbf{F}}_Q(\overline{C})$ que se anulam sobre $\overline{\mathbf{F}}_q$, R é simplesmente a restrição usual de funções, pois como $\overline{\mathbf{F}}_q/\mathbf{F}_q$ é separável , pelo lema 5 da pag 16, não há ramificação.

Pelo teorema 1 do §2 do Cap. I, R é uma aplicação sobrejetora. Além disso, se $\sigma \in G$ então $O_P(\overline{C}) \cap \mathbf{F}_q(\mathbf{C}) = O_{\sigma(P)}(\overline{C}) \cap \mathbf{F}_q(C)$ pois se $f \in \mathbf{F}_q(\mathbf{C})$ está definida em P, f estará definida em $\sigma(P)$ e reciprocamente. Assim, se $G\backslash\overline{V}$ denota o conjunto das órbitas da ação de G em $\overline{V}$, a aplicação R induz uma aplicação $\hat{R}:G\backslash\overline{V} \to V$ que é sobrejetora. Mas $\hat{R}$ é também injetora pois, pelo teorema 2 do §2 do Cap. I, se $v \in V$ e v_1 e v_2 são elementos de $\overline{V}$ que extendem v então existe $\sigma \in G$ tal que $v_1 = v_2 \circ \sigma$. Ou seja, $\hat{R}$ é uma bijeção. O corolário 1 deste § nos garante que há uma correspondência bijetora Φ entre os pontos de $\overline{\mathbf{C}} = C$ e os elementos de $\overline{V}$, dada por $\Phi(P) = O_P(\overline{C})$.

Já vimos que G age naturalmente em $\mathbf{C} = \overline{\mathbf{C}}$ e é fácil ver que Φ comuta com essa ação, isto é

$$\Phi(\sigma(P)) = O_{\sigma(P)}(\overline{C}) = \sigma \cdot O_P(\overline{C}) = \sigma \cdot \Phi(P)$$

e isso implica que Φ leva uma órbita da ação de G em $C = \overline{C}$ numa órbita da ação de G em $\overline{V}$. Assim, se $G\backslash\mathbf{C}$ denota o conjunto dos pontos fechados de C, Φ induz uma bijeção $\hat{\Phi}:G\backslash C \to G\backslash\overline{V}$, donde a composição:

$$G\backslash C \xrightarrow{\hat{\Phi}} G\backslash\overline{V} \xrightarrow{\hat{R}} V$$

é uma aplicação bijetora. C.Q.D.

Se v é uma valorização discreta de um corpo K, $K \supset k$, trivial em k e A_v e M_v são respectivamente o seu anel de valorização e o seu ideal maximal, o corpo A_v/M_v é dito corpo de restos de v (vide §2, Cap. I) e a sua dimensão como k-espaço vetorial é denotada d(v).

Em particular, no nosso caso, se p é um ponto fechado de $\mathbf{C}$ e |p| designa o número de elementos da órbita p, vamos mostrar que a correspondência que leva p na valorização v_p de $\mathbf{F}_q(\mathbf{C})$, trivial sobre $\mathbf{F}_q$, preserva o grau, isto é, $|p| = d(v_p)$.

Seja então p um ponto fechado de $\mathbf{C}$ de tamnaho r ; $|p| = r$, $p = \{P, P^q, \ldots, P^{q^{r-1}}\}$ onde $P = (x_0, x_1, \ldots, x_n) \in \mathbf{P}^n_{\mathbf{F}_{q^m}}$ para certo m. É fácil ver (e será efetivamente provado no lema 1 do §1 do Capítulo IV) que r/m, o que implica que r é o menor inteiro tal que $p \subset \mathbf{P}^n_{\mathbf{F}_{q^r}}$. Assim $O_P(\mathbf{C}) \subset \mathbf{F}_{q^r}(\mathbf{C})$, onde $\mathbf{F}_{q^r}(\mathbf{C})$ é o corpo de funções da variedade $\mathbf{C}$ extendida a $\mathbf{F}_{q^r}$. E portanto temos um morfismo de corpos $O_P(C)/M_P(C) \to \mathbf{F}_{q^r}$ dado pela avaliação em P. Além disso, essa aplicação é $\mathbf{F}_{q^r}$-linear, e portanto é sobrejetora.

Assim $\dim_{\mathbf{F}_q} O_P(C)/M_P(C) = \dim_{\mathbf{F}_q} \mathbf{F}_{q^r} = r$.

CAPÍTULO III

O ENUNCIADO DO TEOREMA DE RIEMANN-ROCH

O teorema de Riemann-Roch é a ferramenta básica para a prova da racionalidade da função zeta, e a originalidade de Stepanov e Bombieri foi sobretudo a utilização engenhosa desse teorema, obtendo assim uma prova "elementar" da Hipótese de Riemann para curvas. Trata-se de um teorema verdadeiramente fundamental e justamente celebrado.

Não faremos aqui uma prova desse teorema, pois para fazê-lo de forma compreensiva necessitariamos de mais espaço do que dispomos, e além disso, se o teorema de Riemann-Roch é essencial para o nosso trabalho, não o é a sua demonstração.

No livro de Fulton, Algebraic Curves, existe uma desmonstração que poderíamos chamar de "clássica" e que, entre outros inconvenientes, considera apenas corpos algebricamente fechadas e se utiliza de um modelo plano da curva projetiva. Isso, além de tornar a prova deselegante e complicada, acarretaria a necessidade de aumentar demasiadamente o capítulo II, tanto no concernente à geometria algébrica quanto à álgebra comutativa.

Já a prova de Chevalley, no seu livro clássico de funções algébricas, é relativamente mais curta e tem a vantagem de considerar corpos arbitrários. Sua única desvantagem é ser incompreensível; pelo menos sem um trabalho complementar que coloque a sua definição de diferencial num contexto adequado. Seguindo de perto Chevaley, Max Deuring (Lectures on the theory of algebraic functions of one variable) repete - com um pouco mais de detalhes - a prova de Chevalley, porém com a mesma definição de diferencial.

Numa outra direção existem as provas de A.Weil (Basic Number Theory) e de Borel e Serre (Le théo-reme de Riemnn-Roch, Bull.Soc.Math. de France 86(1958), pp.97-136) que,apesar de serem as mais curtas, se utilizam de uma maquinaria que não poderíamos desenvolver aqui - como cohomologia de feixes, teoria da dualidade, etc..., de modo que será mais conveniente aos nossos propósitos, simplesmente enunciar,clara e precisamente, o teorema de Riemann-Roch; o que faremos a seguir.

Vimos no capítulo II que se $\mathbf{C}$ é uma curva projetiva não singular definida sobre um corpo finito $\mathbf{F}_q$, então existe uma correspondência bijetora entre os pontos fechados de $\mathbf{C}$ e os anéis de valorização discreta de $\mathbf{F}_q(\mathbf{C})$ que contém $\mathbf{F}_q$, e que se p é um ponto fechado, $|p|$ é igual à dimensão sobre $\mathbf{F}_q$ do corpo de restos da valorização associada à p.

Seja $D(\mathbf{C})$ o grupo abeliano livre gerado pelo conjunto dos pontos fechados de $\mathbf{C}$. Assim um elemento A de $D(\mathbf{C})$ será chamado de divisor de $\mathbf{C}$, e será escrito:

$$A = \sum_p n_p p$$

onde n_p são inteiros quase sempre nulos, isto é nulos exceto para um número finito de pontos fechados. Definimos o grau de um divisor A como $\deg(A) = \sum_p n_p |p|$, e é claro que: $\deg: D(\mathbf{C}) \to Z$ é um homomorfismo de grupos. Dizemos que o divisor $A = \sum_p n_p p$ é efetivo se $n_p \geq 0$ para todo p. Escrevemos $A \geq B$, onde $B = \sum_p m_p p$, se $n_p \geq m_p$ para todo p, ou seja se A-B é efetivo.

PROPOSIÇÃO 1 - Seja $\mathbf{C}$ uma curva projetiva não singular definida sobre $\mathbf{F}_q$. Se $f \in \mathbf{F}_q(\mathbf{C})$, $f \neq 0$, existe apenas um número finito de pontos fechados p, para os quais $v_p(f) \neq 0$, onde v_p é a valorização associada à p.

Para a prova dessa proposição consultar, por exemplo, Deuring, op.cit., pg.24. Com essa proposição, se $f \in \mathbf{F}_q(\mathbf{C})$, $f \neq 0$, podemos associar à f o divisor:

$$(f) = \sum_p v_p(f)p$$

Um divisor $A \in D(\mathbf{C})$ será chamado divisor principal se $A = (f)$ para algum $f \in \mathbf{F}_q(\mathbf{C})$. É claro que o conjunto $D_p(\mathbf{C})$ dos divisores principais é um subgrupo de $D(\mathbf{C})$, e o grupo quociente, $D(\mathbf{C})/D_p(\mathbf{C})$ é chamado o grupo das classes de divisores de $\mathbf{C}$.

Demonstra-se que $\deg((f)) = 0$ (Deuring, pg 27) e portanto a aplicação $\deg: D(\mathbf{C}) \to \mathbf{Z}$ fatoriza-se naturalmente à $\deg: D(\mathbf{C})/D_p(\mathbf{C}) \to \mathbf{Z}$.

Se $A = \sum_p n_p p$ é um divisor de $\mathbf{C}$, definimos o conjunto:

$$L(A) = \{f \in \mathbf{F}_q(\mathbf{C}) : (f) + A \text{ é efetivo}\}$$

Assim $f \in \mathbf{F}_q(\mathbf{C})$ está em $L(A)$ se $v_p(f) \geq -n_p$ ou se $f = 0$. É claro que $L(A)$ é um F_q - espaço vetorial, e denotaremos por $l(A)$ a sua dimensão.

PROPOSIÇÃO 2 - (a) se $A, B \in D(C)$ e $A \leq B$ então $L(A) \subset L(B)$ e $\dim_{\mathbf{F}_q} (L(B)/L(A)) \leq \deg(B-A)$

(b) $L(0) = \mathbf{F}_q$, $L(A) = 0$ se $\deg(A) < 0$

(c) L(A) tem dimensão finita para todo A, e se $\deg(A) \geq 0$ então $l(A) \leq \deg(A) + 1$
(d) Se $A \sim B = (f)$ então $l(A) = l(B)$

Para a demonstração dessa proposição ver Chevalley, (op.cit. pg 14, e pg 21).

Estamos agoram em condições de enunciar o teorema que é conhecido como:

TEOREMA DE RIEMANN. Seja **C** uma curva projetiva não singular sobre $\mathbf{F}_q$. Existe uma constante g tal que $l(A) \geq \deg(A) + 1 - g$ para todos os divisores A. O menor g para a qual a desigualdade acima é verdadeira é chamado o gênero (genus) de **C**, e g é um inteiro não negativo. Além disso existe um inteiro N tal que para todos os divisores A de grau > N,

$$l(A) = \deg(A) + 1 - g.$$

Essa é a contribuição de Riemann ao chamado teorema de Riemann-Roch. Para prova ver Chevalley, pg 21-22.

TEOREMA DE RIEMANN-ROCH. Seja **C** uma curva projetiva não singular sobre um corpo finito $\mathbf{F}_q$. Então existe um divisor K (que depende só de **C**) tal que

$$l(A) = \deg(A) + 1 - g + l(K-A)$$

onde A é um divisor qualquer, g o gênero de **C**.

OBSERVAÇÃO: pondo A = 0 e A = K na equação acima obtemos $l(K) = g$ e $\deg(K) = 2g - 2$. Assim, se $\deg(A) > 2g - 2$, $\deg(K-A) = 2g - 2 - \deg(A) < 0$ donde $l(K-A) = 0$, e assim, se $\deg(A) > 2g - 2$, $l(A) = \deg(A) + 1 - g$.

OBSERVAÇÃO. Se $C/\mathbf{F}_q$ é uma curva projetiva não singular sobre $\mathbf{F}_q$, $f \in \mathbf{F}_q(\mathbf{C})$, e p um ponto fechado de $\mathbf{C}$, dizemos que p é um zero de f se $v_p(f) > 0$ e que p é um polo de f se $v_p(f) < 0$.

CAPÍTULO IV

A HIPÓTESE DE RIEMANN PARA CURVAS SOBRE CORPOS FINITOS

§1 - A Função ZETA de uma Variedade Algébrica

Para maior simplicidade expositiva, neste capítulo faremos algumas modificações na notação e na terminologia até aqui estabelecidas. Se F_q é um corpo finito com q elementos, um ideal $X \subset \mathbf{F}_q[x_1,\ldots,x_N]$ será chamado de variedade afim, e um ideal homogêneo de $\mathbf{F}_q[x_0,x_1,\ldots,x_N]$ será chamado de variedade projetiva. Escrevemos $X/\mathbf{F}_q$ para denotar indistintamente uma variedade afim ou projetiva sobre $\mathbf{F}_q$. Se $X/\mathbf{F}_q$ é uma variedade afim e $L/\mathbf{F}_q$ uma extensão de corpos, definimos:

$$(1) \qquad X(L) = \{(x_1,x_2,\ldots,x_n) \in \mathbf{A}_L^N : f(x_1,\ldots,x_n) = 0, \ \forall\, f \in X\}$$

e de modo análogo definimos X(L) no caso projetivo. Diremos que a variedade $X/\mathbf{F}_q$ é irredutível se X(L) o for, no sentido usual do capítulo II.

O ideal nulo de $\mathbf{F}_q[X_1,X_2,\ldots,X_N]$ será denotado $\mathbf{A}^N$ e o ideal nulo de $\mathbf{F}_q[X_0,X_1,\ldots,X_N]$ será denotado $\mathbf{P}^N$. Com a notação introduzida acima, temos $\mathbf{A}^N(L) = \mathbf{A}_L^N$ e $\mathbf{P}^N(L) = \mathbf{P}_L^N$. Se n é um inteiro ≥ 1, $X/\mathbf{F}_q$ uma variedade sobre $\mathbf{F}_q$ e $L/\mathbf{F}_q$ uma extensão finita de corpos, $|X(L)|$ denotará a cardinalidade de X(L). Se $L = \mathbf{F}_{q^n}$ temos claramente $|\mathbf{A}_L^N| = q^{nN}$ e $|\mathbf{P}_L^N| = \dfrac{q^{n(N+1)} - 1}{q^n - 1}$ e, em particular se $X/\mathbf{F}_q$ é projetiva,

$$|X(L)| \leq \frac{q^{n(N+1)} - 1}{q^n - 1} = 1 + q^n + \ldots + q^{nN}$$

DEFINIÇÃO. Seja $X/\mathbb{F}_q$ uma variedade sobre $\mathbb{F}_q$. Definimos a série formal na variável t:

$$Z(X/\mathbb{F}_q;\ t) = \exp\Big(\sum_{n\geq 1} |X(\mathbb{F}_q n)|\ \frac{t^n}{n}\Big)$$

Essa expressão é chamada de função zeta da variedade $X/\mathbb{F}_q$. Se $Q[[t]]$ designar o anel das séries formais em t com coeficientes racionais, é claro que $Z(X/\mathbb{F}_q;t) \in 1 + t\,Q[[t]]$. Se X for a variedade $\mathbb{A}^N$,

$$Z(\mathbb{A}^N;t) = \exp\Big(\sum_{n\geq 1} |\mathbb{A}^N(\mathbb{F}_q n)|\ \frac{t^n}{n}\Big) =$$

$$= \exp\Big(\sum_{n\geq 1} q^{nN}\ \frac{t^n}{n}\Big) = \frac{1}{1-q^N t}$$

e se X for $\mathbb{P}^N$ teremos:

$$Z(\mathbb{P}^N;t) = \exp\Big(\sum_{n\geq 1} |\mathbb{P}^N(\mathbb{F}_q n)|\ \frac{t^n}{n}\Big) = \exp\Big(\sum_{n\geq 1} \frac{q^{n(N+1)} - 1}{q^n - 1}\ \frac{t^n}{n}\Big)$$

$$= \exp\Big(\sum_{n\geq 1} \sum_{i=0}^{N} \frac{(q^i t)^n}{n}\Big) = \prod_{i=0}^{N} \exp\Big(\sum_{n\geq 1} \frac{(q^i t)^n}{n}\Big)$$

$$= \prod_{i=0}^{N} \frac{1}{1-q^i t}$$

SE $X/\mathbb{F}_q$ é uma variedade arbitrária então $Z(X/\mathbb{F}_q;t)$ define uma função holomorfa na variável complexa t, para $|t| < q^{-N}$. No caso afim isso decorre da (majoração) $|X(\mathbb{F}_q n)| \leq q^{nN}$ e no projetivo, de $|X(\mathbb{F}_q n)| \leq 1+q^n+\ldots+q^{nN}$.

Se fizermos a mudnaça de variável $t = q^{-s}$ e escrevermos:

$$\zeta((X);s) = Z(X/\mathbb{F}_q;q^{-s})$$

segue das considerações acima que $\zeta(X;s)$ é uma série de Dirichlet convergente no semi-plano $Re(s) > N$.

Antes de continuar, relembramos a observação já feita, de que salvo menção contrária, as variedades consideradas serão sempre irredutíveis. Se $X/\mathbb{F}_q$ é uma variedade projetiva não singular de dimensão r definida sobre $\mathbb{F}_q$, temos as "conjecturas de Weil":

(1) Existem 2r+1 famílias de inteiros algébricos $(\alpha_{ji})_{1\leq j\leq B_i}$ $0\leq i\leq 2r$ tais que, se para cada i, $P_i(t) = \prod_{j=1}^{B_i} (1-\alpha_{ji}t)$ então

$$Z(X/\mathbb{F}_q;t) = \frac{P_1(t)\ P_3(t)\ \ldots\ P_{2r-1}(t)}{P_o(t)\ P_2(t)\ \ldots\ P_{2r}(t)}$$

e além disso $P_o(t) = 1-t$ e $P_{2r}(t) = 1-q^r t$.

(2) (Equação Funcional). Se pusermos $x = \sum_{i=0}^{2r} (-1)^i B_i$ então:

$$Z(X/\mathbb{F}_q;\ \frac{1}{q^r t}\ ) = \pm\ q^{rx/2}\ t^x\ Z(X/\mathbb{F}_q;t)$$

(3) (Hipótese de Riemann). Para todo par de índices j,i tem-se

$$|\alpha_{ij}| = q^{i/2}$$

(4) (Racionalidade dos "polinômios de Weil"). Cada um dos polinômios P_i tem coeficientes inteiros racionais, de termo constante igual à 1.

Se X for uma curva projetiva não singular definida

sobre $\mathbb{F}_q$, temos, em particular

$$(1') \qquad Z(X/\mathbb{F}_q;t) = \frac{P(t)}{(1-t)\,(1-qt)}$$

onde P(t) é um polinômio com coeficientes inteiros racionais de grau 2g (g é o gênero da curva), coeficiente dominante igual a q^g e termo constante 1.

(2') (Equação Funcional). P(t) satisfaz a equação funcional

$$P(1/qt) = q^{-g}\, t^{-2g}\, P(t)$$

(3') (Hipótese de Riemann). Os zeros de P(t) têm módulo $q^{-1/2}$.

OBSERVAÇÕES (1): Decorre de (2) acima que a função zeta para curvas verifica:

$$Z(X/\mathbb{F}_q;1/qt) = q^{1-g}\, t^{2-2g}\, Z(X/\mathbb{F}_q;t)$$

(2) Se fizermos a mudança de variável $t = q^{-s}$, podemos reescrever (3') acima, pondo que os zeros de $\zeta(X;s)$ estão sobre a reta

$$Re(s) = \frac{1}{2}$$

Ao longo do trabalho veremos que enquanto (1') e (2') são consequências quase diretas do teorema de Riemann-Roch, a Hipótese de Riemann para curvas, (3'), embora também decorra desse teorema, é bem mais difícil de deduzir.

No capítulo II consideramos a ação natural de $Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ sobre $X(\bar{\mathbb{F}}_q)$ e chamamos de ponto fechado a uma ór

bita dessa ação. Vimos também - pelas considerações que se seguem a proposição 6 do capítulo I - que todo ponto fechado possui um número finito de elementos. Se p é um ponto fechado de grau r, e fácil ver que cada um dos elementos de p está em $\mathbf{A}^r_{\mathbb{F}_q r}$ ou $\mathbb{P}^r_{\mathbb{F}_q r}$, conforme X seja afim ou projetiva. Assim, se $B_n(X)$ designar o número de pontos fechados de $X(\bar{\mathbb{F}}_q)$ de grau n, $B_n(X)$ é finito.

LEMA 1. Se $X/\mathbb{F}_q$ é uma variedade sobre $\mathbb{F}_q$ então

$$|X(\mathbb{F}_q n)| = \sum_{r|n} r\, B_r(X)$$

PROVA. Seja $a \in X(F_q n)$, $a = (x_1, x_2, \ldots, x_N)$ no caso afim, ou $a = (x_0, x_1, \ldots, x_N)$ no caso projetivo, tal que sua órbita $\{a, a^q, a^{q^2}, \ldots, a^{q^{r-1}}\}$ tenha r elementos. No caso afim, temos $x_j{}^{q^r} = x_j$, $j = 1,2,\ldots,N$. Se todos os x_j forem nulos, então $r=1$ e $1|n$. Se os x_j não forem todos nulos então existe um certo $x_j \neq 0$ cujo período (em $\mathbb{F}_q^* n$) é exatamente q^r-1, serão a órbita de a não poderia ter tamanho r, e assim $x_j \in \mathbb{F}_q r$, mas então x_j é um gerador de $\mathbb{F}_q^* r$, donde $\mathbb{F}_q r \subset \mathbb{F}_q n$ e pela proposição 2 do capítulo I, $r|n$.

No caso projetivo, $x_j^{q^r} = \lambda\, x_j$, $j = 0,1,\ldots,N$.

Se x_i é um elemento não nulo da classe a,

então $(\frac{x_j}{x_i})^{q^r} = \frac{x_j}{x_i}$, $j = 0,1,\ldots,N$, donde $\frac{x_j}{x_i} \in \mathbb{F}_q r$ e o resto é análogo.

Agora, decompondo $X(\mathbb{F}_q n)$ como reunião disjunta de suas órbitas e aplicando a definição de $B_r(X)$, obtemos:

$$|X(\mathbb{F}_q n)| = \sum_{r \leq n} r\, B_r(X).$$

Mas acabamos de provar que se $X(\mathbb{F}_q n)$ possui uma órbita de tamanho r, então r|n. C.Q.D.

TEOREMA 1. Seja $X/\mathbb{F}_q$ uma variedade sobre $\mathbb{F}_q$. Então

$$Z(X/\mathbb{F}_q;t) = \prod_p \frac{1}{(1-t^{|p|})}$$

onde o produto é tomado sobre todos os pontos fechados de $X(\bar{\mathbb{F}}_q)$.

PROVA: Tomando a derivada logarítmica de $Z(X/\mathbb{F}_q;t)$ e aplicando o lema 1 obtemos:

$$\frac{Z'(X/\mathbb{F}_q;t)}{Z(X/\mathbb{F}_q;t)} = \sum_{n\geq 1} \Big(\sum_{r|n} r\, B_r(X) \Big) t^{n-1} = \sum_{n\geq 1} \Big(\sum_{\{p:|p|\,|\,n\}} |p| \Big) t^{n-1}$$

$$= \sum_{n\geq 1} \sum_p |p| t^{m|p|-1} = \sum_p \frac{|p| t^{|p|-1}}{(1-t^{|p|})}$$

$$= \sum_p \frac{[(1-t^{|p|})^{-1}]'}{[(1-t^{|p|})^{-1}]} = \Big(\sum_p \log(1-t^{|p|})^{-1} \Big)'$$

$$= [\log Z(X/\mathbb{F}_q;t)]' = [\log \prod_p \frac{1}{(1-t^{|p|})}]'$$

donde

$$Z(X/\mathbb{F}_q;t) = k. \prod_p \frac{1}{(1-t^{|p|})}$$

como $Z(X/\mathbb{F}_q;0) = 1$, temos $k = 1$.

C.Q.D.

Se $X/\mathbb{F}_q$ é uma variedade sobre $\mathbb{F}_q$ e $L/\mathbb{F}_q$ é uma extensão de corpos, podemos pensar na variedade $X \otimes L/L$ obtida por extensão de escalares, como fizemos no capítulo II. Relembramos que $X \otimes L$ é o ideal gerado por X em $L[X_1, X_2, \ldots, X_N]$ ou em $L[X_0, X_1, \ldots, X_N]$. É claro que, na nova notação,

$$(X \otimes L)\ (E) = X(E),$$

para uma extensão E/L.

PROPOSIÇÃO 1. Seja d um inteiro ≥ 1 e $X/\mathbb{F}_q$ uma variedade definida sobre $\mathbb{F}_q$. Então:

$$Z(X \otimes \mathbb{F}_{q^d}/\mathbb{F}_{q^d}; t^d) = \prod_{\{\zeta:\ \zeta^d = 1\}} Z(X/\mathbb{F}_q; \zeta\, t)$$

PROVA: Seja θ um gerador do grupo das raízes d-ésimas da unidade e n um inteiro ≥ 1. Então

$$\theta^n \Big(\sum_{\{\zeta:\zeta^d=1\}} \zeta^n \Big) = \sum_{\zeta} (\theta\,\zeta)^n = \sum_{\zeta} \zeta^n$$

donde segue que

$$(\theta^n - 1) \Big(\sum_{\zeta} \zeta^n \Big) = 0$$

Assim, se $d \nmid n$, $\theta^n \neq 1$ e portanto $\sum_{\zeta} \zeta^n = 0$.

Se $d|n$, $\zeta^n = 1$ e $\sum \zeta^n = d$. Vamos aplicar essas observações à função:

$$\prod_{\{\zeta\ \zeta^d=1\}} \exp\Big(\sum_{n\geq 1} |X(\mathbb{F}_q n)| \frac{(\zeta t)^n}{n} \Big) =$$

$$= \exp\Big(\sum_{\zeta} \sum_{n\geq 1} |X(\mathbb{F}_q n)| \frac{(\zeta t)^n}{n} \Big)$$

A proposição estará provada se mostrarmos que

$$\sum_{n\geq 1} |X(\mathbb{F}_q nd)| \frac{t^{nd}}{n} = \sum_{\zeta} \sum_{n\geq 1} |X(\mathbb{F}_q n)| \frac{\zeta^n t^n}{n}$$

Mas

$$\sum_{\zeta} \sum_{n\geq 1} |X(\mathbb{F}_q n)| \frac{\zeta^n t^n}{n} = \sum_{n\geq 1} |X(\mathbb{F}_q n)| \frac{t^n}{n} \Big(\sum \zeta^n \Big) =$$

$$= \sum_{m\geq 1} |X(\mathbb{F}_q md)| \frac{t^{md}.d}{md}$$

C.Q.D.

§2 - A Função ZETA de Curvas Algébricas

Neste parágrafo consideraremos sempre uma curva projetiva não singular $\mathbf{C}/\mathbf{F}_q$ definida sobre $\mathbf{F}_q$. O teorema 1 nos permite escrever

$$Z(\mathbf{C}/\mathbf{F}_q;t) = \prod_p \frac{1}{1-t^{|p|}} = \prod_p (1+t^{|p|}+t^{2|p|}+\ldots)$$

$$= \sum_{n\geq 0} A_n t^n$$

onde $A_o=1$ e A_n é o número de divisores efetivos de grau n, para $n \geq 1$.

Se E_n designa o conjunto dos divisores efetivos de grau n e S_n é um conjunto de representantes das classes de divisores de grau n, temos

$$E_n = \bigcup_{A\in S_n} \{ B: B \text{ é efetivo, } B \equiv A(\text{mod } D_p(\mathbf{C})) \}$$

ou seja,

$$E_n = \bigcup_{A\in S_n} \{ A+(f) : A+(f) \text{ é efetivo} \} =$$

$$= \bigcup_{A\in S_n} \{A+(f) : f \in L(A),\ f \neq 0\}$$

Mas

$$|\{A+(f) : f \in L(A);\ f\neq 0\}| = |\{(f) : f \in L(A),\ f\neq 0\}|$$

e como $(f) = (g)$ se e só se $f=kg$ para algum $k \in \mathbb{F}_q^*$, então

$$|\{(f): f \in L(A),\ f\neq 0\}| = \frac{|\{f: f \in L(A),\ f\neq 0\}|}{q-1}$$

e

$$\frac{|\{f: f \in L(A),\ f\neq 0\}|}{q-1} = \frac{q^{l(A)}-1}{q-1}$$

donde

$$A_n = \sum_{A \in S_n} \frac{q^{l(A)}-1}{q-1}$$

e podemos escrever a função zeta como:

$$(q-1)\ Z(\mathbb{C}/\mathbb{F};t) = \sum_{n\geq 0} t^n \sum_{A\in S_n} (q^{l(A)}-1).$$

Embora seja evidente, é bom observar que das considerações acima decorre a finitude do número de classes de divisores de grau n, $|S_n|$. É importante notar também que $|S_n|$ = constante, para todo $n \geq 1$, pois se A_o é um divisor de grau n_o, a aplicação $A+D_p(\mathbb{C}) \to A+A_o+D_p(\mathbb{C})$ é uma bijeção entre o conjunto das classes de divisores de grau n e o conjunto das classes de divisores de grau $n+n_o$. No que segue, $|S_n| = h$, $n \geq 1$.

Para obter mais informações sobre $h = |S_n|$, precisamos estudar a imagem do morfismo de grupos deg: $D(\mathbf{C}) \to \mathbf{Z}$. Seja $d\mathbf{Z}$ o subgrupo de $\mathbf{Z}$ que é a imagem do homomorfismo deg. Então se A_o é um divisor cujo grau é d e A é um divisor arbitrário, $\deg(A) = m.\deg(A_o)$ para algum $m \in \mathbf{Z}$, donde

$$d = m.d.c.\{\deg(A) : A \in D(\mathbf{C})\}$$

ou seja, $d = m.d.c\{|p| : p \text{ é ponto fechado}\}$. Vamos mostrar que d=1. Seja n um inteiro ≥ 0. Se $d \nmid n$ então não existem divisores de grau n, e se $d|n$, já sabemos que $|S_n| = h$ e a função zeta fica:

$$(q-1)\, Z(\mathbf{C}/\mathbf{F}_q;t) = \sum_{n\geq 0} t^{nd} \sum_{A\in S_{nd}} q^{l(A)} - \sum_{n\geq 0} t^{nd} h$$

$$= \sum_{n\geq 0} t^{nd} \sum_{A\in S_{nd}} q^{l(A)} - \frac{h}{1-t^d}$$

Se K é o divisor canônico (cf. Cap.III), já vimos que $\deg(K) = 2g-2$ e portanto d divide 2g-2 e a função zeta pode ser reescrita:

$$(q-1)\, \mathbf{Z}(\mathbf{C}/\mathbf{F};t) = \sum_{n=0}^{(2g-2)/d} t^{nd} \sum_{A\in S_{nd}} q^{l(A)} +$$

$$+ \sum_{n>(2g-2)/d} t^{nd} \sum_{A\in S_{nd}} q^{l(A)} - \frac{h}{1-t^d}$$

Mas se $A \in S_{nd}$ e $\deg(A) = nd > 2g-2$, sabemos que

$$l(A) = \deg(A) + 1-g = nd+1-g,$$

donde

$$(q-1)\, Z(\mathbf{C}/\mathbf{F}_q;t) = \sum_{n=0}^{(2g-2)/d} t^{nd} \sum_{A \in S_{nd}} q^{l(A)} +$$

$$+ \sum_{n>(2g-2)/d} t^{nd}\, q^{nd+1-g}\, h - \frac{h}{1-t^d}$$

ou seja:

$$(*) \qquad (q-1)\, Z(\mathbf{C}/\mathbf{F}_q;t) = \sum_{n=0}^{(2g-2)/d} t^{nd} \sum_{A \in S_{nd}} q^{l(A)} +$$

$$+ \frac{h q^{1-g}\, (tq)^{2g-2+d}}{1-t^d q^d} - \frac{h}{1-t^d}$$

PROPOSIÇÃO 1: Seja p um ponto fechado de $\mathbf{C}/\mathbf{F}_q$ de grau $|p|$. Se $l \mid |p|$, podemos pensar em $p \otimes \mathbf{F}_q l$ como um ponto fechado de $\mathbf{C} \otimes \mathbf{F}_q l/\mathbf{F}_q l$. Então $|p \otimes \mathbf{F}_q l| = |p|/l$.

PROVA: Seja $r = |p|$. Então p está contido em $\mathbf{C}(\mathbf{F}_q r)$. O estabilizador de um elemento $a \in p$ é o sugrupo $G(\bar{\mathbf{F}}_q/\mathbf{F}_q r)$ e portanto $r = |G(\bar{\mathbf{F}}_q/\mathbf{F}_q)/G(\bar{\mathbf{F}}_q/\mathbf{F}_q r)|$, pela toeria elementar das ações de grupos. Como $l \mid r$, $\mathbf{F}_q l \subset \mathbf{F}_q r$ e o estabilizador de $p \otimes \mathbf{F}_q l$ é $G(\bar{\mathbf{F}}_q/\mathbf{F}_q r)$. Logo $|p \otimes \mathbf{F}_q l| = |G(\bar{\mathbf{F}}_q/\mathbf{F}_q l)/G(\bar{\mathbf{F}}_q/\mathbf{F}_q r)| = \dim_{\mathbf{F}_q l} \mathbf{F}_q r = \frac{r}{l} = \frac{|p|}{l}$ C.Q.D.

A expressão (*) foi obtida para uma curva projetiva não singular $\mathbf{C}/\mathbf{F}_q$, onde d era o gerador da imagem do homomor

fismo deg:D($\mathbf{C}$) → $\mathbf{Z}$. Façamos agora uma extensão de escalres para $\mathbf{F}_q d$, considerando a curva $\mathbf{C} \times \mathbf{F}_q d/\mathbf{F}_q d$. Seja $\bar{d}$ o gerador da imadem de $D(\mathbf{C} \otimes \mathbf{F}_q d)$ em Z. Pela proposição 1, $\bar{d} = 1$. A fórmula (*) aplicada à $\mathbf{C} \otimes \mathbf{F}_q d$ dá:

$$(q^d-1)\ \mathbb{Z}(\mathbf{C} \otimes \mathbf{F}_q d/\mathbf{F}_q d;t) = \sum_{n=0}^{2g-2} t^n \sum_{A \in S_n} q^{d\ell(A)}$$

$$+ \frac{\bar{h}.q^{d(1-g)}\ t^{2g-1}\ q^{d(2g-1)}}{1-tq^d} - \frac{\bar{h}}{1-h}$$

e no ponto t^d obtemos:

$$(q^d-1)\ \mathbf{Z}(\mathbf{C} \otimes \mathbf{F}_q d/\mathbf{F}_q d;t^d) = \sum_{n=0}^{2g-2} t^{nd} \sum_{A \in S_n} q^{dl(A)} +$$

$$+ \frac{\bar{h}.q^{d(1-g)}\ t^{d(2g-1)}\ q^{d(2g-1)}}{1-t^d q^d} - \frac{\bar{h}}{1-t^d}$$

Assim $Z(\mathbf{C} \otimes \mathbf{F}_q d/\mathbf{F}_q d;t^d)$ possui um polo simples em t=1. Mas já vimos que

$$Z(\mathbf{C} \otimes \mathbf{F}_q d/\mathbf{F}_q d;t^d) = \prod_{\{\zeta:\zeta^d=1\}} Z(\mathbf{C}/\mathbf{F}_q;\zeta t)$$

e portanto, da expressão (*), é imediato que

$$Z(\mathbf{C}/\mathbf{F}_q;\zeta\, t) = Z(\mathbf{C}/\mathbf{F}_q;t) \text{ e}$$

$$Z(\mathbf{C} \otimes \mathbf{F}_q d/\mathbf{F}_q d;t^d) = [Z(\mathbf{C}/\mathbf{F}_q;t)]^d$$

Como $Z(\mathbf{C}/\mathbf{F}_q;t)$ tem um polo simples em t=1, $Z(\mathbf{C} \otimes \mathbf{F}_q d/\mathbf{F}_q d;t^d)$

terá um polo simples em t=1 se e só se d=1. Assim podemos reescrever a função zeta:

$$(q-1)\ Z(\mathbf{C}/\mathbf{F}_q;t) = \sum_{n=0}^{2g-2} t^n \sum_{A \in S_n} q^{l(A)} +$$

$$+ \frac{h.q^g t^{2g-1}}{1-qt} - \frac{h}{1-t}$$

ou seja:

$$Z(\mathbf{C}/\mathbf{F}_q;t) = \frac{P(t)}{(1-t)\ (1-qt)}$$

onde P(t) é um polinômio de grau 2g, e P(0) = 1. Vamos mostrar que o grau de P(t) é 2g. Para tanto vamos reescrever explicitamente a expressão geral da função zeta:

$$(q-1)\ Z(\mathbf{C}/\mathbf{F}_q;t) = b_0+b_1t+\ldots+b_{2g-2}t^{2g-2} + \frac{h\ q^g\ t^{2g-1}}{1-qt} - \frac{h}{1-t}$$

onde

$$b_i = \sum_{A \in S_i} q^{l(A)}$$

PROPOSIÇÃO 2. Para $0 \leq i \leq 2g-2$, $b_i\ q^{g-1-i} = b_{2g-2-i}$.

PROVA: Já sabemos que se deg(A) = i, então

$$\deg(K-A) = 2g-2-i.$$

Assim, se $S_i = \{A_1,\ldots,A_h\}$ então $\{K-A_1,\ldots,K=A_h\}$ é um conjunto de representantes de classes de divisores de grau 2g-2-i, isto é, $\{K-A_1,\ldots,K-A_h\} = S_{2g-2-i}$. Assim, se

$b_i = \sum_{j=1}^{h} q^{l(A_j)}$, então $b_{2g-2-i} = \sum_{j=1}^{h} q^{l(K-A_j)}$

Mas pelo teorema de Riemann-Roch,

$$l(A_j) = i+1-g+l(K-A_j), \text{donde temos,}$$

$$b_{2g-2-i} = \sum_{j=1}^{h} q^{l(A_j)-i-1+g} = q^{g-1-i}\, b_i$$

C.Q.D.

Se pusermos t=0 na expressão geral da função zeta, como $\mathbf{Z}(\mathbf{C}/\mathbf{F}_q;0) = 1$, segue

$$(q-1)\ \mathbf{Z}(\mathbf{C}/\mathbf{F}_q;0) = b_o - h, \text{ donde } b_o = q-1+h$$

e portanto $b_{2g-2} = q^{g-1}\ (h+q-1)$. Decorre daí que o termo independente de P(t) é 1 e o coeficiente de ordem 2g é:

$$\frac{q\ b_{2g-2} - hq^g}{(q-1)} = \frac{q^g(h+q-1) - hq^g}{(q-1)} = q^g$$

donde o grau de P(t) é 2g e o coeficiente dominante é q^g.

PROPOSIÇÃO 3. (Equação Funcional) Se $\mathbf{C}/\mathbf{F}_q$ é uma curva projetiva não singular sobre $\mathbf{F}_q$, então

$$\mathbf{Z}(\mathbf{C}/\mathbf{F}_q;\tfrac{1}{qt}) = q^{1-g}\, t^{2-2g}\, \mathbf{Z}(\mathbf{C}/\mathbf{F}_q;t)$$

PROVA: Substituindo t por 1/qt na expressão geral da função zeta obtemos:

$$(q-1)\ \mathbf{Z}(\mathbf{C}/\mathbf{F}_q;\tfrac{1}{qt}) = b_o + \frac{b_1}{qt} + \ldots + \frac{b_{2g-2}}{q^{2g-2}\ t^{2g-2}} +$$

$$+ \frac{hq^g}{q^{2g-1}\ t^{2g-1}} \cdot \frac{1}{(1-1/t)} - \frac{h}{1-1/qt}$$

$$= b_o + \frac{b_1}{qt} + \ldots + \frac{b_{2g-2}}{q^{2g-2}\ t^{2g-2}} - \frac{q^g h}{q^{2g-1}\ t^{2g-2}(1-t)} + \frac{qth}{(1-qt)}$$

$$= q^{1-g}\ t^{2-2g} \left[b_o q^{g-1}\ t^{2g-2} + b_1 q^{g-2}\ t^{2g-3} + \ldots + q^{1-g}\ b_{2g-2} \right] -$$

$$- \frac{q^{1-g}\ t^{2-2g}\ h}{(1-t)} + \frac{q^g\ t^{2g-1}\ h\ q^{1-q}\ t^{2-2g}}{(1-qt)}$$

$$= q^{1-g}\ t^{2-2g} \left[(b_{2g-2}\ t^{2g-2} + \ldots + b_o) + \frac{h\ q^g\ t^{2g-1}}{1-qt} - \frac{h}{1-t} \right]$$

$$= q^{1-g}\ t^{2-2g}\ \mathbf{Z}(\mathbf{C}/\mathbf{F}_q;t).$$

C.Q.D.

Podemos escrever a função zeta como:

$$\mathbf{Z}(\mathbf{C}/\mathbf{F}_q;t) = \frac{\prod_{i=1}^{2g} (1-\alpha_i t)}{(1-t)\ (1-qt)}$$

onde os α_i são os inversos dos zeros de P(t).

A equação funcional para $Z(\mathbf{C}/\mathbf{F}_q;t)$ implica imediatamente:

$$P(t) = q^g \, t^{2g} \, P\left(\frac{1}{qt}\right)$$

e portanto se $1/\alpha_i$ é raiz, α_i/q também será raiz de $P(t)$.

COROLÁRIO 1. Valem as igualdades:

$$h = -\frac{\prod_{i=1}^{2g} (1-\alpha_i)}{(1-q)} \qquad \text{e} \qquad \prod_{i=1}^{2g} \alpha_i = q^g$$

PROVA: A primeira igualdade exprime simplesmente o fato de que $-h$ é o resíduo da função zeta no polo $t = 1$. A segunda igualdade segue do fato de que o coeficiente dominante de $P(t)$ é q^g.

Precisamos mostrar que os α_i são inteiros algébricos. Ora, provamos que $Z(\mathbf{C}/\mathbf{F}_q;t)$ é uma função racional em t com coeficientes inteiros. Sabemos que $Z(\mathbf{C}/\mathbf{F}_q;0) = 1$ e que o desenvolvimento em série de potências $Z(\mathbf{C}/\mathbf{F}_q;t) = \sum_{n\geq 0} A_n t^n$ tem coeficientes inteiros.

Há um teorema, devido a Fatou (Acta Math., 30, pp 364-400) que diz o seguinte: se $F(t)$ é uma função racional com coeficientes em Q, se $F(0) = 1$ e se o desenvolvimento em série de Taylor de $F(t)$ possui todos os coeficientes inteiros, então os zeros e polos de $F(t)$ são inversos de inteiros algébricos. Isso mostra que os α_i são inteiros algébricos.

PROPOSIÇÃO 4. Se $\mathbf{C}/\mathbf{F}_q$ é uma curva projetiva não-singular sobre $\mathbf{F}_q$ e $\mathbf{C} \otimes \mathbf{F}_q n/F_q n$ denota a curva obtida pela extensão de escalares à $\mathbf{F}_q n$, então:

$$\mathbf{Z}(\mathbf{C} \otimes \mathbf{F}_q n/\mathbf{F}_q n; t) = \frac{\prod_{i=1}^{2g} (1-\alpha_i^n)}{(1-t)(1-q^n t)}$$

PROVA: Já vimos que a função zeta pode ser escrita como:

$$Z(\mathbf{C}/\mathbf{F}_q; t) = \frac{\prod_{i=1}^{2g} (1-\alpha_i t)}{(1-t)(1-qt)}$$

e além disso,

$$Z(\mathbf{C} \otimes \mathbf{F}_q n/\mathbf{F}_q n; t^n) = \prod_{\{\zeta^n=1\}} Z(C/F_q; \zeta t) = \frac{\prod_{\zeta} \prod_{i=1}^{2g} (1-\alpha_i \zeta t)}{\prod_{\zeta} (1-\zeta t)(1-q\zeta t)}$$

Mas $1-t^n = \prod_{\zeta} (1-\zeta t)$, donde

$$Z(\mathbf{C} \otimes \mathbf{F}_q n/\mathbf{F}_q{}^n; t^n) = \frac{\prod_{i=1}^{2g} (1-\alpha_i^n t^n)}{(1-t^n)(1-q^n t^n)}$$

e segue a proposição. C.Q.D.

COROLÁRIO 1. Se $Z(\mathbf{C}/\mathbf{F}_q; t) = \prod_{i=1}^{2g} (1-\alpha_i t)/(1-t)(1-qt)$ então

$$|\mathbf{C}(\mathbf{F}_q n)| = 1 + q^n - \sum_{i=1}^{2g} \alpha_i^n$$

PROVA. Fazendo uma extensão de escalares à $\mathbf{F}_q n$, e aplicando a proposição 4 segue:

$$\frac{\prod_{i=1}^{2g} (1-\alpha_i^n t)}{(1-t)(1-q^n t)} = \exp\left(\sum_{k \geq 1} |\mathbf{C}(\mathbf{F}_q nk)| \frac{t^k}{k} \right) =$$

$$= 1 + |\mathbf{C}(\mathbf{F}_q n)|t + \ldots$$

Por outro lado,

$$\prod_{i=1}^{2g} (1-\alpha_i^n t)(1+t+t^2+\ldots)(1+q^n t+q^{2n}t^2+\ldots) =$$

$$= 1 + (1+q^n - \sum_{i=1}^{2g} \alpha_i^n)t + \ldots$$

igualando as duas séries obtemos:

$$|\mathbf{C}(\mathbf{F}_q n)| = 1 + q^n - \sum_{i=1}^{2g} \alpha_i^n$$

C.Q.D

§3 - PROVA DA HIPÓTESE DE RIEMANN PARA CURVAS

O trabalho preliminar já foi feito, e vamos agora provar a "hipótese de Riemann" para curvas, isto é, que

$$|\alpha_i| = q^{1/2}$$

ou equivalentemente, os zeros de $\zeta(\mathbf{C};S)$ estão sobre a reta $\mathrm{Re}(s) = \frac{1}{2}$.

Suponhamos por um isntante que essa "hipótese" seja verdadeira, isto é, que $|\alpha_i| = q^{1/2}$.

como

$$|\mathbf{C}(\mathbf{F}_q n)| = 1 + q^n - \sum_{i=1}^{2g} \alpha_i^n \quad \text{temos}$$

$$||\mathbf{C}(\mathbf{F}_q n)| - 1 - q^n| \leq \sum_{i=1}^{2g} |\alpha_i|^n = 2g\, q^{n/2}$$

No próximo lema provaremos que qualquer desigualdade do tipo acima é equivalente à "hipótese de Riemann".

LEMA 1. Suponhamos que exista um número $A > 0$ tal que para todo $n \geq 1$,

$$||\mathbf{C}(\mathbf{F}_q n)| - 1 - q^n| \leq A\, q^{n/2}$$

Então vale a "hipótese de Riemann".

PROVA: Por hipótese $\left| \sum_{i=1}^{2g} \alpha_i^n \right| \leq A\, q^{n/2}$

Consideremos a função:

$$\sum_{i=1}^{2g} \frac{1}{1-\alpha_i t} = \sum_{i=1}^{2g} \sum_{n=0}^{\infty} (\alpha_i t)^n = \sum_{n=0}^{\infty} \left(\sum_{i=1}^{2g} \alpha_i^n \right) t^n$$

A série acima é majorada por $A \sum_{n=0}^{\infty} q^{n/2} |t|^n$, e esta última converge para $|t| < q^{-1/2}$.

Logo, os polos $1/\alpha_i$ da função $\sum_{i=1}^{2g} \frac{1}{1-\alpha_i t}$ devem estar fora do disco de raio $q^{-1/2}$, isto é,

$$q^{-1/2} \leq |\alpha_i|^{-1}, \quad \text{ou seja,} \quad |\alpha_i| \leq q^{1/2}$$

Mas como $\prod_{i=1}^{2g} |\alpha_i| = q^g = (q^{1/2})^{2g}$, segue necessariamente a igualdade $|\alpha_i| = q^{1/2}$

C.Q.D.

Assim, para estabelecermos a validade da "hipótese de Riemann" é suficiente provarmos que $||\mathbf{C}(\mathbf{F}_q n)| - 1 - q^n| \leq A\, q^{n/2}$ para todo $n \geq 1$ e para certo $A > 0$. Na realidade, não precisamos provar essa desigualdade para todo $n \geq 1$ pois em virtude da proposição 4 do §2, a "hipótese de Riemann" para a curva $\mathbf{C}$ sobre $\mathbf{F}_q$ é equivalente à "hipótese de Riemann" para a curva extendida $\mathbf{C} \otimes \mathbf{F}_q n$ sobre $\mathbf{F}_q n$. Assim, podemos supor sem nenhuma perda de generalidade que $n = 1$, $q > (g+1)^4$, $q = p^a$ com a par. Ou seja, a constante A que encontraremos não depende do corpo de base.

O próximo teorema, cuja demonstração é devida à Stepanov-Bombier, dá conta da "metade" da "hipótese de Riemann". A outra "metade", que segue de um raciocínio de cahomologia goloisiana, seguirá adiante.

TEOREMA 1. Se $\mathbf{C}/\mathbf{F}_q$ é uma curva projetiva não singular sobre F_q, de gênero g, com $q > (g+1)^4$, $q = p^a$, a par então:

$$|\mathbf{C}(\mathbf{F}_q)| \leq 1 + q + (2g+1)q^{1/2}$$

PROVA: Evidentemente podemos supor $\mathbf{C}(\mathbf{F}_q) \neq \emptyset$, pois caso contrário $|\mathbf{C}(\mathbf{F}_q)| = 0$. Seja então $p \in \mathbf{C}(\mathbf{F}_q)$. p é um ponto fechado de grau 1, isto é, um ponto fixo de $\mathbf{C}(\bar{\mathbf{F}}_q)$ pela ação de $\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$. Seguindo Bombieri, consideraremos a curva C extendida ao fecho algébrico $\mathbf{F}_q$, i.e, $\mathbf{C} \otimes \bar{\mathbf{F}}_q/\bar{\mathbf{F}}_q$ (ou, $\bar{\mathbf{C}}/\bar{\mathbf{F}}_q$).

Seja $L_m = \{f \in \bar{\mathbf{F}}(\bar{\mathbf{C}}) : v_p(f) \geq -m\}$ e l_m a dimensão de L_m como $\mathbf{F}_q$ - espaço vetorial.

Temos $\bar{F}_q = L_o \subset L_1 \subset \ldots \subset L_m \subset \ldots$ e as propriedades abaixo:

(1) $l_m \geq m + 1 - g$ e, se $m > 2g - 2$, então $l_m = m + 1 - g$

(Isso é simplesmente o teorema da Riemann, que enunciamos na pg.44).

(2) $l_{m+1} \leq 1 + l_m$. (Do teorema de Riemann-Roch, $l_{m+1} - l_m = 1 + l(K-(m+1)p) - l(K-mp)$, e como $L(K-(m+1)p) \subseteq L(K-mp)$, então $l_{m+1} - l_m \leq 1$).

(3) Se $f(X) \in L_m$ então $f(X^q) \in L_{mq}$.
(Isso simplesmente diz que se $f(X)$ tem em p um polo de ordem $\leq m$, então $f(X^q)$ terá em p um pelo de ordem $\leq mq$).

(4) Existe uma base $\{f_1,\ldots,f_r\}$ de L_m tal que $v_p(f_i) < v_p(f_{i+1})$ para $i = 1,2,\ldots,r-1$, pois temos a filtração

$$(0) \subset \bar{F}_q = 1_o \subset L_1 \subset \ldots \subset L_m \quad e$$

portanto

$$L_m \tilde{=} \bigoplus_{i=0}^{m} L_i/L_{i-1}$$

Mas decorre da propriedade (2) que $\dim L_i/L_{i-1} \leq 1$, o que implica (4) pois para cada i, quando for possível, tomamos um elemento de L_i que não esteja em L_{i-1}.

Sejam agora n,b inteiros não negativos e sejam $S_1,\ldots,S_r$ elementos de L_n.

Consideremos a função auxiliar:

$$F(X) = S_1^{p^b}(x)\, f_1(x^q) + \ldots + S_n^{p^b}(x)\, f_n(x^q)$$

(5) Se $np^b < q$, temos que $F(x)$ é identicamente nulo se e só se todos os S_i forem identicamente nulos.
De fato, suponhamos que $F(x)$ seja identicamente nulo e que $S_h(x)$ seja o primeiro S_i não identicamente nulo. Tomando v_p em ambos os lados da identidade:

$$S_h^{p^b}(x)\, f_h(x^q) = - S_{h+1}^{p^b}(x)\, f_{h+1}(x^q) - \ldots -$$

$$- S_r^{p^b}(x)\, f_r(x^q)$$

obtemos,

$$p^b\, v_p(S_h) + q\, v_p(f_h) \geq \min_{i>h}(p^b\, v_p(S_i) +$$

$$+ q\, v_p(f_i)) \geq - p^b n + q\, v_p(f_{h+1})$$

e portanto

$$p^b\, v_p(S_h) \geq -p^b n + q(v_p(f_{h+1}) - v_p(f_h))$$

ou seja, por (4),

$$p^b\, v_p(S_h) \geq - p^b n + q > 0$$

donde segue que S_h se anula em p, e portanto é uma função sem polos com pelo menos um zero, ou seja, $v_p(S_h) > 0$ e $v_q(S_h) \geq 0$ para todo $q \neq p$.
Como $\sum_p v_p(S_h) = 0$, segue que $S_h \equiv 0$.

(6) Se $m,n > 2g-2$ e se $(n+1-g)(m+1-g) > p^b n + m + 1 - g$ então podemos escolher os S_i não todos identicamente nulos tal que a função

$$S_1^{p^b}(x)\, f_1(x) + \ldots + S_r^{p^b}(x)\, f_r(x)$$

seja identicamente nula.

De fato, essa função é regular fora de p e tem em p um polo cuja ordem é $\leq p^b n + m$.

Logo, por (1), o conjunto dessas funções forma um $\bar{\mathbb{F}}_q$-espaço vetorial de dimensão $\leq p^b n + m + 1 - g$.

Como cada S_i varia num espaço de dimensão $n + 1 - g$ e como, $r = m + 1 - g$ (pois $m > 2g-2$), e por hipótese $(n+1-g)(m+1-g) > p^b n + m + 1 - g$ a aplicação canônica

$$L_n^{p^b} \underset{\bar{\mathbb{F}}_q}{\otimes} L_m \longrightarrow L((p^b n+m)p)$$

não pode ser injetora; o que prova (6).
(Observe que $\dim L_n = \dim L_n^{pb}$)
Assim, em vista de (5) e (6), obtemos que, se $m,n > 2g-2$, $np^b < q$,

$(n+1-g)(m+1-g) > np^b + m + 1 - g$, podemos construir uma função auxiliar

$$F(X) = S_1^{p^b}(x)\, f_1(x^q) + \ldots + S_r^{p^b}(x)\, f_r(x^q)$$

não identicamente nula e tal que se $a \in \mathbb{C}(\mathbb{F}_q)$ $a \neq p$, então $F(a) = 0$ (note que $a^q = a$).

Ou seja, F se anula em todos os pontos de $\mathbf{C}(\mathbb{F}_q)$ exceto em p. Como $p^b < q$, por construção, vemos que F(x) é uma potência p^b-ésima, isto é, $F(x) = G(x)^{p^b}$ para certa $G(x) \in \bar{\mathbb{F}}_q(\bar{\mathbf{C}})$ e assim cada zero de F(x) tem multiplicidade pelo menos p^b. Logo F(x) tem pelo menos $p^b(|\mathbf{C}(\mathbb{F}_q)| - 1)$ zeros. Logo

$$(|\mathbf{C}(\mathbb{F}_q)| - 1) \leq \frac{1}{p^b} \#(\text{zeros de } F) =$$

$$= \frac{1}{p^b} \#(\text{polos de } F) \leq$$

$$\leq \frac{1}{p^b}(p^b\, n+mq)$$

pois F é resular fora de p e a ordem do polo em p não pode exceder $p^b n+mq$.

Resumindo, até agora vimos que se $m,n > 2g-2$, $np^b < q$ e $(n+1-g)(m+1-g) > np^b+m+1-g$,

então

$$|\mathbf{C}(\mathbf{F}_q)| \leq 1 + n + \frac{mq}{p^b}$$

Tomando $p^b = q^{1/2}$, $n=q^{1/2}-1$, $m=q^{1/2}+2g$ e lembrando que, por hipótese, $q > (g+1)^4$

(a) $n = q^{1/2}-1 > (g+1)^2-1 = g^2+2g > 2g-2$

(b) $m = q^{1/2}+2g > 2g-2$

(c) $(n+1-g)(m+1-g) = (p^b-g)(p^b+2g+1-g) =$

$= (p^b-g)(p^b+g+1) = p^bp^b+p^bg+p^b-gp^b-g^2-g$

$= p^bp^b+p^b-g-g^2 > p^bp^b+g^2+2g+1-g-g^2 =$

$= p^bp^b+1+g = np^b+m+1-g$

(d) Como $(q^{1/2}-1)q^{1/2} < q$, $np^b < q$.

Assim, todas as condições estão verificadas e portanto

$$|\mathbf{C}(\mathbf{F}_q)| \leq 1 + (q^{1/2}-1) + \frac{(q^{1/2}+2g)q}{q^{1/2}}$$

ou seja:

$$|\mathbf{C}(\mathbf{F}_q)| \leq 1 + q^{1/2}-1 + q+2gq^{1/2}$$

$$\leq 1 + q + (2g+1)q^{1/2}$$

C.Q.D.

Resta agora provar a outra "metade" da hipótese de Riemann, pois o argumento acima não nos dá uma limitação inferior para $|\mathbf{C}(\mathbf{F}_q)|$.

Por exemplo, se $|\mathbf{C}(\mathbf{F}_{q^r})| = 1 + q^r - \alpha_1^r - \alpha_2^r$ e $\alpha_1 = q$, $\alpha_2 = 1$, então $\alpha_1 \alpha_2 = q$, $|\mathbf{C}(\mathbf{F}_{q^r})|$ é sempre zero, mas é falso que $|\alpha_i| = q^{1/2}$. A idéia básica para provar o que falta, é fazer um raciocínio de contagem sobre uma família de corpos conjugados, de uma extensão fixa de um corpo dado. A parte abstrata do raciocínio é o seguinte lema de contagem do número de pontos fixos da ação de um grupo finito num conjunto dado.

Seja G um grupo finito, H um subgrupo de G, $N_G(H)$ o normalizador de H em G e σ um elemento fixo de $N_G(H)$. Seja X um conjunto onde G age e $x \in X$. A órbita de x pela ação de G será denotada $O_G(x)$ e o conjunto das órbitas da ação de G em X será escrito $G\backslash X$.

Como H é subgrupo de G, H age em X pela restrição da ação de G, e como $\sigma \in N_G(H)$, σ induz uma aplicação $\hat{\sigma}$: $H\backslash X \to H\backslash X$ dada por $\hat{\sigma} \cdot O_H(x) = O_H(\sigma x)$. É imediato que $\hat{\sigma}$ está bem definida. Se $g \in G$, Fix(g) denota o conjunto dos $x \in X$ tais que $gx = x$ e, como sempre, |Fix(g)| denota a cardinalidade de Fix(g).

PROPOSIÇÃO 1. Com as hipóteses e notações acima vale:

$$\sum_{h \in H} |\mathrm{Fix}(\sigma h)| = |H| . |\mathrm{Fix}(\hat{\sigma})|$$

PROVA: Seja $A = \bigcup_{h \in H} \mathrm{Fix}(\sigma h)$ e a seguinte relação de equivalência em A: $x \sim y$ se $O_H(x) = O_H(y)$. É imediato que se $x \in A$, $O_H(x) \subset A$ e $O_H(x) \in \mathrm{Fix}(\hat{\sigma})$, donde segue que $A/\sim = \mathrm{Fix}(\hat{\sigma})$. Queremos computar $\sum_{h \in H} |\mathrm{Fix}(h)|$. Se $x \in A$, x é contado $|H_x|$ vezes

onde H_x é o estabilizador de x em H, e portanto $O_H(x) \in A/\sim$ contribui com $|H:H_x| . |H_x|$ vezes, pois os estabilizadores de elementos da mesma órbita são conjugados.

Assim, cada elemento de $A/\sim$ é contado em $\sum_{h \in H} |fix(\sigma h)|$, $|H|$ vezes, donde

$$|Fix(\hat{\sigma})| = |A/\sim| = \frac{1}{|H|} \sum_{h \in H} |Fix(\sigma h)|$$

C.Q.D.

Retornando ao problema original, seja k um corpo finito com q elementos, K/k um corpo de funções algébricas de uma variável sobre k e L/K uma extensão de Galois finita. Podemos considerar K como o corpo de funções racionais de uma curva C/k. Designamos por $V_1(K/k)$ o conjunto das valorizações discretas de K que se anulam em k e cujo corpo de restos tem grau 1 sobre k.

Já vimos no capítulo II que se C/k é uma curva projetiva não singular sobre k, que existe uma correspondência bijetora entre os pontos fechados de grau 1 de C e os elementos de $V_1(K/k)$.

Vamos agora provar o teorema 1, abaixo, que nos permitirá completar a prova da "hipótese de Riemann". A prova que fizemos foi baseada em notas de um seminário da Karl Otto Stöhr.

TEOREMA 2. Seja k um corpo finito com q elementos, K/k um corpo de funções algébricas de uma variável e L/K uma extensão uma extensão de Galois finita. Além disso suponhamos que k seja algebricamente fechado em L. Então existem [L:K] corpos de funções algébricas de uma variável, L_t/k, $t \in Gal(L/K)$ verificando:

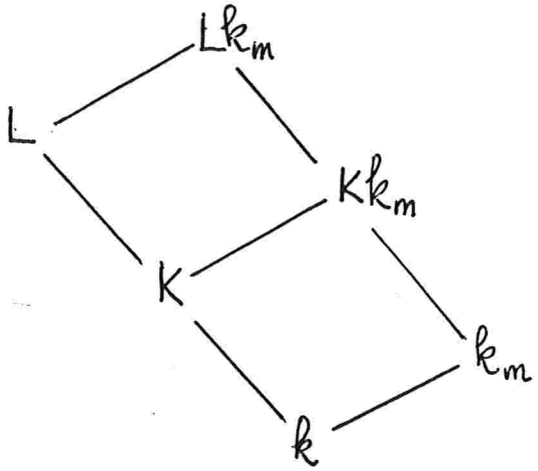
(a) $L_{id} = L$

(b) $L_t \supset K$ e $[L_t:K] = [L:K]$

(c) $L_t.\bar{k} = L.\bar{k}$, onde $\bar{k}$ é um fecho algébrico de k

(d) $\sum_{t \in G(L/K)} |V_1(L_t/k)| = [L:K].|V_1(K/k)|$

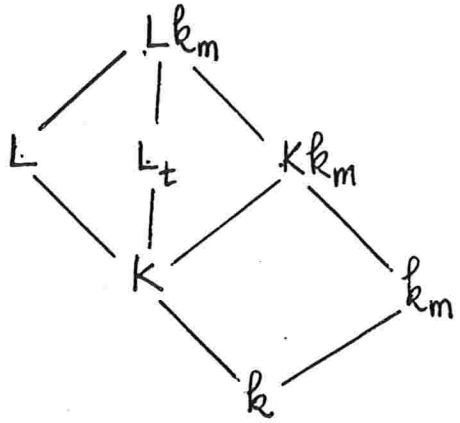
PROVA. Seja $m = [L:K]$ e k_m/k uma extensão de grau m. Como $L \cap k_m = k$, $G(k_m/k) \simeq G(Kk_m/K) \simeq G(Lk_m/L)$, e



como $L \cap Kk_m = K$, então $G(L/K) \simeq G(Lk_m/Kk_m)$. Vimos no capítulo I que G(km/k) é cíclico e gerado pelo automorfismo de Frobenius $S:a \longmapsto a^q$. Seja σ o automorfismo induzido por S em $G(Lk_m/L)$. Se $t \in G(L/K)$, seja τ o automorfismo induzido por t em $G(Lk_m/Kk_m)$. É claro que $\sigma\tau$ é um automorfismo de Lkm sobre k e que $\sigma\tau = \tau\sigma$. Como o período de σ é m e o τ de divide m se f for o período de $\sigma\tau$ então f divide m. Mas se $x \in km$, $(\sigma\tau)^f(x) = S^f(x) = x$ donde m divide f, e portanto m = f, ou seja, a ordem de $\sigma\tau$ é precisamente m.

Seja $L_t = \{a \in Lk_m : (\sigma\tau)a = a\}$ o corpo fixo pelo grupo gerado por $\sigma\tau$. Pela toeria de Galois a exten

são Lk_m/L_t é de Galois finita com grupo de Galois $\langle\sigma\tau\rangle$, ou seja $|Lk_m: L_t| = m$.



Decorre daí que L_t/k é um corpo de funções algébricas de uma variável sobre k. Além disso, $L_tk_m = Lk_m$ pois como $L_t \subset Lk_m$, $L_tk_m \cap Lk_m$ e além disso:

$$L_t \cap k_m = \{a \in k_m: (\sigma\tau)a = a\} = \{a \in k_m: S(a) = a\} = k$$

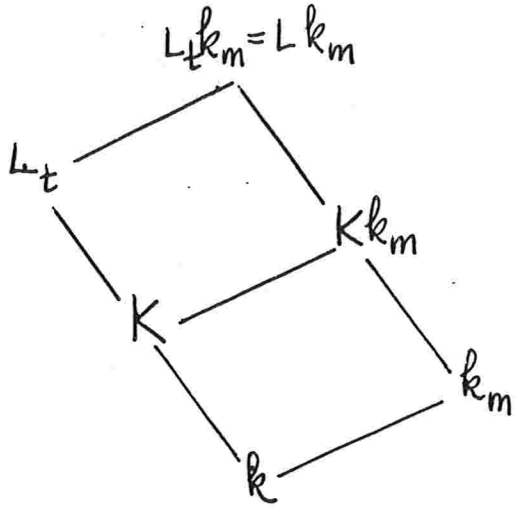
donde

$$|Lk_m:L_t] = m \quad \text{e assim } L_tk_m = Lk_m.$$

Note-se que $L_t\bar{k} = (L_tk_m)\bar{k} = (Lk_m)\bar{k} = L\bar{k}$.

Como $L \cap Kk_m = K$, temos da teoria de Galois que $G(Lk_m/K) \simeq G(L/K) \times G(Kk_m/K)$, e portanto podemos pensar em $G(L/K)$ como subgrupo de $G(Lk_m/K)$.

Vamos agora nos utilizar dos resultados acerca de valorização para compararmos certos cardinais de conjuntos de valorizações. Consideremos a seguinte situação:



onde já vimos que $G(k_m/k) \simeq G(L_t k_m/L_t)$.

O grupo $G(Lkm/K)$ age naturalmente em $V(Lk_m/k_m)$ - - o conjunto das valorizações discretas de Lk triviais em k_m. A ação é dada por $\Psi.v \to v\circ\Psi^{-1}$. Como $G(L_t k_m/L_t)$ é subgrupo de $G(Lk_m/K)$, podemos pensar na ação desse subgrupo por restrição da ação de $G(Lk_m/K)$.

Se $v \in V(L_t k_m/k_m)$, depois do lema 5, § 2, Cap. I, podemos considerar a restrição usual de funções para obtermos uma valorização $v|_{L_t} \in V(L_t/k)$ ou seja, temos uma aplicação:

$$\text{Rest: } V(L_t k_m/k_m) \longrightarrow V(L_t/k)$$

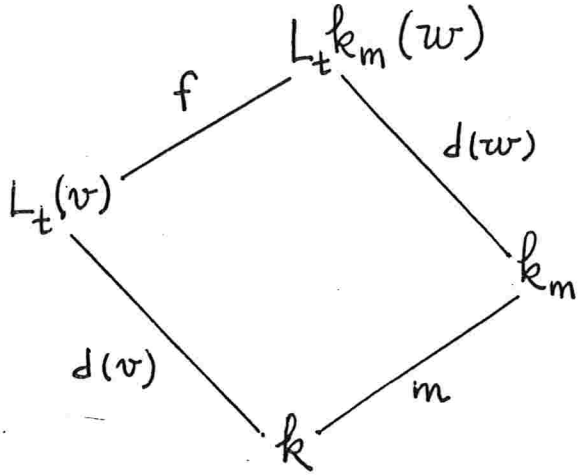
dada pela restrição usual de funções. Pelo teorema 1, § 2, Cap. I, rest é uma aplicação sobrejetora.

Já vimos também (teor.2, §2, Cap.I) que se $v \in V(L_t/k)$, $\text{Rest}^{-1}(v)$ é uma órbita da ação de $H_t = G(L_t k_m/L_t)$ em $V(Lk_m/k_m)$. Assim existe um correspondên

cia bijetora entre $V(L_t/k)$ e as órbitas $H_t \backslash V(L_t k_m/k_m)$.

Vamos agora provar que há uma correspondência bijetora entre $V_1(L_t/k_m)$ e $Fix(H_t)$ onde $Fix(H_t) = \{v \in V_1(L_t k_m/k_m) : v o \rho^{-1} = v, \forall\ \rho \in H_t\}$.

Seja então $v \in V(L_t/k)$ e $L_t(v)$ o seu corpo de restos ($L_t(v) = A_v/M_v$). Seja $d(v)$ a sua dimensão como k-espaço vetorial. Pela prop.1, §2, Cap.I, $d(v)$ é finito. Se $w \in V(L_t k_m/k_m)$ é uma extensão de v temos: o diagrama:



Se $g = |O_{H_t}(w)|$, isto é, é o número de extensões de v à $L_t k_m$, pelo teorema 3, §2, Cap.I, sabemos que $e.f.g = m$, donde $d(v)f = d(w)fg$, pois $e = 1$ (Lema 5, §2, Cap.I), ou seja, $d(v) = g\, d(w)$.

Logo se $w \in Fix(H_t)$, sua órbita tem tamanho 1, donde $w|_{L_t} = v$ tem $d(w|_{L_t}) = 1$.

Reciprocamente, se $v \in V_1(L_t/k)$ e w extende v, então $1 = g\, d(w)$, donde $g = 1$ e $d(w) = 1$.

Assim:

$$V_1(L_t/k) = \{ w\big|_{L_t} : w \in Fix(H_t)\}$$

Como $H_t = \langle\sigma\tau\rangle$, é claro que

$$|V_1(L_t/k)| = |Fix(H_t)| = |Fix(\sigma\tau)|$$

Pondo $G = G(Lk_m/K)$, $H = G(L/K)$ e $X = V_1(Lk_m/k_m)$, como $\sigma t = t\sigma$ para todo $t \in G(L/K)$, $\sigma \in (N_G(H)$ e pela proposição 1 deste §,

$$\frac{1}{[L:K]} \sum_{t\in G(L/K)} |V_1(L_t/k)| = \frac{1}{|H|} \sum_{t\in H} |Fix(\sigma t)| =$$

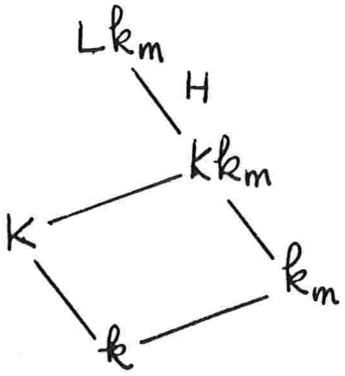
$$= |Fix(\hat{\sigma})|$$

onde $\hat{\sigma}$ é a aplicação induzida nas órbitas de $G(L/K)$ em $V_1(Lk_m/k_m)$.

Resta mostrar que $|Fix(\hat{\sigma})| = |V_1(K/k)|$:

$$\hat{\sigma} : \frac{V_1(Lk_m/k_m)}{H} \longrightarrow \frac{V_1(Lk_m/k_m)}{H}$$

é dada por $O_H(v) \longmapsto O_H(v\circ\sigma^{-1})$



Como $H = G(L/K) \simeq G(Lk_m/Kk_m)$, temos na mesma situação da pg. 77, ou seja,

$$|\mathrm{fix}(\hat{\sigma})| = |V_1(K/k)|$$

Isso prova (d),

C.Q.D.

Observe-se que se $K = k(X)$ for o corpo de funções racionais (isto é, K é o corpo de funções da variedade projetiva $\mathbf{P}^1_{\mathbf{F}_q}$) então o número de pontos fechados de grau 1, é precisamente

$$\frac{q^2-1}{q-1} = q+1,$$

e portanto

$$\sum_{t \in G(L/k(X))} |V_1(L_t/K)| = [L:k(X)]\,(q+1)$$

É importante observar também que se $\mathbf{C}/\mathbf{F}_q$ é uma curva projetiva não singular sobre $\mathbf{F}_q$ e $K = \mathbf{F}_q(\mathbf{C})$ é o corpo de funções racionais em $\mathbf{C}$, então é possível encontrar um elemento θ transcendente sobre $\mathbf{F}_q$ tal que a extensão $K/\mathbf{F}_q(\theta)$ seja separável (cf.Iyanaga, Theory of numbers, p.34). Assim, podemos tomar uma extensão $L/\mathbf{F}_q(\theta)$ que seja de Galois finita e que contenha K, por exemplo $L = K^{nor}$, o fecho normal de K sobre $\mathbf{F}_q(\theta)$. O que não se pode garantir a priori é que $\mathbf{F}_q$ seja algebricamente fechado em L. Para contornar esse problema, seja k' o fecho algébrico de $\mathbf{F}_q$ em L.

Como $L/\mathbf{F}_q$ é uma extensão finitamente gerada e $L \supset k' \supset \mathbf{F}_q$, $k'/\mathbf{F}_q$ será finitamente gerada, e como é algébrica, decorre que $k'/\mathbf{F}_q$ é finita. Assim podemos fazer uma ex

tensão de escalares $C \otimes k'/k'$ e provar a hipótese de Riemann sobre k'.

TEOREMA 3. Se $\mathbf{C}/\mathbf{F}_q$ é uma curva projetiva não singular sobre $\mathbf{F}_q$, de gênero g, com $q > (g+1)^4$, $q = p^a$, a par, $K = \mathbf{F}_q(\mathbf{C})$ o corpo de funções racionais de $\mathbf{C}$ e L/K uma extensão de Galois finita com $\mathbf{F}_q$ algebricamente fechado em L então existe $A > 0$ tal que

$$||\mathbf{C}(\mathbf{F}_q)| - 1 - q| \leq A\, q^{1/2}$$

PROVA: O teorema 1 deste parágrafo nos deu

$$|\mathbf{C}(\mathbf{F}_q)| - 1 - q \leq (2g+1)\, q^{1/2}$$

Aplicando esse mesmo teorema à família de corpos de funções algébricas de uma variável $L_t/\mathbf{F}_q$ obtemos:

$$|V_1(L_t/\mathbf{F}_q)| \leq (q+1) + (2g_L+1)\, q^{1/2}$$

onde g_L é o gênero da curva associada à extensão $L/\mathbf{F}_q$. Assim, se $S \notin G(L/\mathbf{F}_q(\theta))$ temos:

$$\sum_{\substack{t \in G(L/\mathbf{F}_q(\theta)) \\ t \neq S}} |V_1(L_t/\mathbf{F}_q)| \leq ([L:\mathbf{F}_q(\theta)] - 1)\ [(q+1) + (2g_L+1)q^{1/2}]$$

e

$$|V_1(L_S/\mathbf{F}_q)| = [L:\mathbf{F}_q(\theta)]\,(q+1) - \sum_{t \neq S} |V_1(L_t/\mathbf{F}_q)|$$

Pondo $[L:\mathbf{F}_q(\theta)] = n$ vem:

$$|V_1(L_S/\mathbf{F}_q)| \geq n(q+1) - (n-1)\,[(q+1) + (2g_L+1)\,q^{1/2}]$$

$$\geq (q+1) - (n-1)\,(2g_L+1)\,q^{1/2}$$

donde

$$\sum_{S \in G(L/K)} |V_1(L_S/\mathbf{F}_q)| \geq [L:K][(q+1) - (n-1)(2g_L+1)\,q^{1/2}]$$

e portanto

$$|V_1(K/\mathbf{F}_q)| \geq (q+1) - (n-1)\,(2g_L+1)\,q^{1/2}$$

tomando $A = \max\{(2g+1), (n-1)(2g_L+1)\}$

segue que

$$||\mathbf{C}(\mathbf{F}_q)| - 1 - q| \leq A\,q^{1/2}$$

C.Q.D.

BIBLIOGRAFIA

[1] : E.Artin. Collected Papers. Springer Verlag

[2] : Atiyah e Macdonald. Introduction to Commutative Algebra. Adolison - Wesley (1969)

[3] : E.Bombieri. Counting Points on Curves over finite fields. Séminaire Bourbaki 1973 nº 430

[4] : W.Fulton. Algebraic Curves. W.A. Benjamin, Inc. 1969

[5] : R.Hartshorne. Algebraic Geometry. Springer-Verlag G.M.T. vol.52.