Seminário: Teorias O-minimais e Geometria Algébrica Real

Ricardo Bianconi

1^o Semestre de 2010

O Teorema de Harnack

1 Introdução

Este texto nasce de uma série de seminários visando preparar alunos de pós graduação para trabalhar nesse tema.

O texto a seguir não sofreu nenhuma revisão e, por isso, deve ser lido com muito cuidado, corrigindo os erros que porventura escaparem.

Assumiremos que, exceto menção explícita em contrário, todos os aneis e corpos são de característica zero.

2 O Resolvente

Sejam K um corpo e $p, q \in K[x]$ dois polinômios. O problema que queremos resolver é decidir se ambos tem uma solução comum, em alguma extensão de K. Isto pode ser exprimido como a busca de um fator comum $h \in K[x]$, não constante, para p e q. Escrevendo $p(x) = h(x)p_1(x)$ e $q(x) = h(x)q_1(x)$, podemos recolocar o problema como a procura de polinômios $p_1, q_1 \in K[x]$, cujos graus sejam menores que os de p e q, respectivamente, e tais que $q_1(x)p(x) = p_1(x)q(x)$.

Escrevendo [1] $p(x) = \sum_{i=0}^{n} a_i x^i$, $q(x) = \sum_{i=0}^{m} b_i x^i$, $p_1(x) = \sum_{i=0}^{n-1} u_i x^i$ e $q_1(x) = \sum_{i=0}^{m-1} v_i x^i$, o problema reduz-se a determinarmos se existem $u_0, \ldots, u_{n-1}, v_0, \ldots, v_{m-1} \in K$, sendo que nem todos sejam nulos, de modo a obtermos a igualdade $q_1(x)p(x) = p_1(x)q(x)$, ou $q_1(x)p(x) - p_1(x)q(x) = 0$.

[1] Renomeando os polinômios, se necessário, podemos supor que $n \geq m$.

Para que isso ocorra, os coeficientes de todos os monômios do polinômio do lado esquerdo da igualdade devem anular-se:

Coeficiente de $1 = x^0$: $a_0v_0 - b_0u_0 = 0$.

Coeficiente de x: $a_1v_0 + a_0v_1 - b_1u_0 - b_0u_1 = 0$

$\vdots$

Coeficiente de x^k: $\sum_{i=0}^{k} a_{k-i}v_i - \sum_{i=0}^{k} b_{k-i}u_i = 0$, para $k \leq m-1 \leq n-1$.

Coeficiente de x^k: $\sum_{i=0}^{k} a_{k-i}v_i - \sum_{i=k-m}^{k} b_{k-i}u_i = 0$, para $m \leq k \leq n-1$.

Coeficiente de x^k: $\sum_{i=k-n}^{m-1} a_{k-i}v_i - \sum_{i=k-m}^{n-1} b_{k-i}u_i = 0$, para $n \leq k \leq m+n-1$.

Isto pode ser expresso na forma matricial (pois é um sistema linear nas variáveis $v_0, \ldots, v_{m-1}$ e $(-u_0), \ldots, (-u_{m-1})$ (essa troca de sinal é pura conveniência):

$$M \begin{pmatrix} v_0 \\ \vdots \\ v_{m-1} \\ -u_0 \\ \vdots \\ -u_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

A matriz dos coeficientes do sistema linear é:

$$M = \begin{pmatrix} a_0 & 0 & 0 & \ldots & 0 & 0 & b_0 & 0 & 0 & \ldots & 0 & 0 \\ a_1 & a_0 & 0 & \ldots & 0 & 0 & b_1 & b_0 & 0 & \ldots & 0 & 0 \\ a_2 & a_1 & a_0 & \ldots & 0 & 0 & b_2 & b_1 & b_0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & a_n & a_{n-1} & 0 & 0 & 0 & \ldots & b_m & m-1 \\ 0 & 0 & 0 & \ldots & 0 & a_n & 0 & 0 & 0 & \ldots & 0 & b_m \end{pmatrix}$$

A matriz dos coeficientes desse sistema linear tem $n+m$ linhas e colunas, sendo que as primeiras m colunas contem apenas os coeficientes de $p(x)$ e zeros, enquanto que as n últimas contem apenas os coeficientes de $q(x)$ e zeros.

Esse sistema admite uma solução não trivial se, e somente se, o determinante da matriz dos coeficientes do sistema linear se anular. Esse determinante é chamado de resolvente de p e q, e denotado por $R(p, q)$. O resultado final que desejamos é:

Teorema 2.1 (Resolvente) Dados os polinômios $p(x) = \sum_{i=0}^{n} a_i x^i$ e $q(x) = \sum_{i=0}^{m} b_i x^i$ em $K[x]$ $(1 \leq m \leq n)$, então o resolvente $R(p,q)$ anula-se se, e somente se, ou $a_n = b_m = 0$ ou eles admitem um fator comum não constante.

3 O Teorema de Bézout para curvas

Agora o problema que queremos resolver é determinar o número máximo de pontos de uma intersecção de duas curvas planas, dadas pelo sistema $p(x,y) = 0$, $q(x,y) = 0$, com $p, q \in K[x,y]$, desde que essa intersecção seja finita.

Suponhamos que exista apenas uma quantidade finita de soluções para o sistema $p(x,y) = q(x,y) = 0$. Então se $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(K)$ for matriz invertível, então a quantidade de soluções do sistema acima é a mesma que a do sistema $p(ax+by, cx+dy) = q(ax+by, cx+dy) = 0$. Como o corpo K é infinito, e a quantidade de soluções do sistema é finita, então existe pelo menos uma matriz como acima tal que, para cada $x \in K$, existe no máximo um $y \in K$, tal que(x,y) é solução do novo sistema. Podemos, então, assumir que o sistema original possui essa propriedade.

Considerando p, q como elementos de $K(x)[y]$ (polinômios em y, com coeficientes em $K(x)$, podemos aplicar o critério do resolvente, obtendo $R(p,q)$, um polinômio em x, de grau igual ao produto dos graus (totais) de p e q (observe que a diagonal da matriz do resolvente contém m vezes o elemento a_0 e n vezes o elemento b_m; como a_0 é um polinômio em x de grau igual ao de $p(x,y)$ e b_m é de grau zero em x, o grau de $R(p,q)$ é esse mesmo). Assim, temos o

Teorema 3.1 (Bézout) Suponha que a quantidade de soluções do sistema $p(x,y) = q(x,y) = 0$ seja finita, sendo que $p, q \in K[x,y]$. Então essa quantidade não é maior do que o produto dos graus totais dos polinômios p e q.

4 Curvas algébricas planas

4.1 Topologica das curvas simples e fechadas no plano projetivo

O plano projetivo (sobre um corpo $\mathbb{K}$) pode ser definido como o conjunto de todas as retas de $\mathbb{K}^3$ passando pela origem (ou seja, todas as soluções em

$\mathbb{K}^3$ de equações lineares homogêneas não triviais).

No caso em que $\mathbb{K}$ tem uma topologia natural (por exemplo, se for um corpo ordenado, herdando a topologia definida pela ordem), o plano projetivo admitirá uma topologia compatível, herdada de $\mathbb{K}^3$: é a topologia menos fina que torna a projeção $\pi : \mathbb{K}^3 \to \mathbb{P}_2(\mathbb{K})$ contínua.

Podemos visualizar a topologia do plano projetivo (real) da seguinte forma. Seja $\mathbb{K}$ um corpo ordenado. Considere a esfera unitária $S^2 = \{(x, y, z) \in \mathbb{K}^3 : x^2 + y^2 + z^2 = 1\}$, com a topologia induzida de $\mathbb{K}^3$. Então o plano projetivo pode ser visto como o quociente de S^2 pela relação de equivalência $p \sim q$ se $p = q$ ou $p = -q$ (antípoda). A topologia de $\mathbb{P}_2(\mathbb{K})$ é gerada pelas projeções dos abertos de S^2. Um conjunto de representantes dessas classes de equivalência pode ser o conjunto $X = \{(x, y, z) \in S^2 : z > 0$, ou $(z = 0$ e $y \geq 0\} \setminus \{(0, 0, -1)\}$.

Na figura 1, vemos o hemisfério superior da esfera. Aí fica fácil visualizar o fato de que o plano projetivo consiste de uma faixa de Möbius colada a um disco.

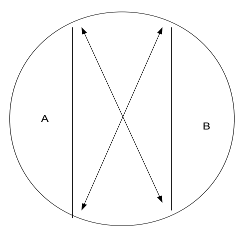

Figura 1: Hemisfério supoerior da esfera visto de cima.

Uma curva simples e fechada no plano projetivo real (os casos em que $\mathbb{K}$ for um outro corpo ordenado será tratado em outra ocasião) pode ser de dois tipos: ou é uma **pseudo-reta**, que é uma deformação cotínua de uma reta projetiva, e, portanto, seu complemento é homeomorfo a um plano afim; ou é uma **oval**, ou seja, seu complemento no plano projetivo consiste de duas "componentes", o interior, que é homeomorfo a um disco, e seu exterior, que é homeomorfo a uma faixa de Möbius.

Uma curva algébrica não singular no plano projetivo não pode ter mais de uma componente pseudo-reta,pois o complemento de uma pseudo-reta será homeomorfo a um plano afim e neste todas as curvas simples e fechadas são ovais (dividem o "plano afim"em duas partes: o interior e o exterior da curva.

4.2 O Teorema de Harnack

Vamos aplicar o Teorema de Bézout para delimitar o número de componentes conexas de uma curva projetiva plana real.

Vamos tratar aqui do caso em que o corpo $K = \mathbb{R}$, deixando para mais adiante sua generalização para qualquer corpo real fechado.

Uma curva não singular do plano projetivo é o conjunto solução (em coordenadas homogêneas de $\mathbb{P}_2(\mathbb{R})$) de um polinômio homogêneo $p(x, y, z) \in \mathbb{R}[x, y, z]$ não constante, tal que o vetor $(\partial p/\partial x, \partial p/\partial y, \partial p/\partial z)$ não se anule em nenhum ponto da curva.

Observemos que uma curva algébrica de grau N no plano projetivo é definida por um polinômio homogêneo não trivial de grau N, da forma

$$p(x, y, z) = \sum_{0 \leq i+j \leq N} a_{i,j} x^i y^j z^(N - i - j),$$

sendo que nem todos os coeficientes $a_{i,j}$ são nulos. Estes coeficientes perfazem um total de $(N + 1)(N + 2)/2$ elementos e, portanto, podemos fazer uma bijeção entre curvas definidas por tais polinômios e elementos do espaço projetivo $\mathbb{P}_{(N+1)(N+2)/2}(\mathbb{R})$.

Se escolhermos pontos $\xi_k \in \mathbb{P}_2(\mathbb{R})$, $1 \leq k \leq M$, com coordenadas homogêneas (ou seja, triplas ordenadas em $\mathbb{R}^3 \setminus \{(0, 0, 0)\}$), "em posições genéricas", considerando os coeficientes $a_{i,j}$ de $p(x, y, z)$ como variáveis, o sistema linear $p(\xi_k) = 0$, $1 \leq k \leq M$ terá a matriz dos coeficientes com posto $\min\{M, (N + 1)(N + 2)/2\}$. Portanto, se $M \geq (N + 1)(N + 2)/2$, o sistema linear admitirá somente a solução nula. Portanto, para garantirmos a possibilidade de existir uma curva algébrica de grau N passando pelos pontos dados, M deverá ser no máximo $(N + 1)(N + 2)/2 - 1$.

Teorema 4.1 (Harnack) Uma curva algébrica não singular do plano projetivo real, de grau n, possui não mais que $g(n) + 1$ componentes conexas, sendo $g(n) = (n - 2)(n - 1)/2$.

Demonstração: Os casos $n = 1$ e $n = 2$ são simples. Podemos considerar o caso $n > 2$.

Suponhamos que exista uma curva não singular de grau $n > 2$ com pelo menos $L = g(n) + 2$ componentes, $\Gamma_1, \ldots, \Gamma_L$. Então, no máximo uma dentre elas pode ser uma pseudo-reta. Digamos que $\Gamma_1, \ldots, \Gamma_{L-1}$ sejam todas ovais.

Se fizermos $N = n - 2$, para determinarmos uma curva de grau N, podemos escolher $(N+1)(N+2)/2 - 1 = n(n-1)/2 - 1$ pontos no plano projetivo. Como $n > 2$, temos que $n(n-1)/2 - 1 \geq g(n) + 1$. Se escolhermos "genericamente"pontos $\xi_k \in \Gamma_k$, para $1 \leq k \leq L - 1 = g(n) + 1$, e os restantes $\xi_k \in \Gamma_L$, $g(n)+2 \leq k \leq n(n-1)/2 - 1$, temos que, para cada oval, a intersecção da nova curva com a oval contém pelo menos mais um ponto (a curva entra e sai da oval) e, portanto teremos pelo menos $2(L-1) + n(n-1)/2 - g(n) - 2 = g(n) + n(n-1)/2 = (n-1)^2$ pontos de intersecção.

Por outro lado, o Teorema de Bézout diz que não poderia haver mais do que $n(n-2) = n^2 - 2n$ pontos, uma contradição à quantidade $n^2 - 2n + 1$ de pontos obtidos. $\square$