NOTAS DE AULA DO

PICME

Programa de Iniciação Científica e Mestrado em Combinatória

http://www.ime.usp.br/~tcco/picme

Anotado por: Marcelo Sales

2º semestre de 2017

Conteúdo

1 Nullstellensatz Combinatório

◇ ◇ ◇ *Aula 1 (15 de Agosto) — Yoshiharu Kohayakawa* ◇ ◇ ◇

Nessa seção vamos tratar de teoremas sobre zeros em conjuntos de polinômios. Para fins combinatórios estamos normalmente interessados em corpos finitos, porém iniciaremos a teoria considerando corpos quaisquer. Seja $\mathbb{K}$ um corpo e $\mathbb{K}[X_1, \ldots, X_n]$ o anel de polinômios de n variáveis em $\mathbb{K}$. Dado uma familia $\mathcal{F}$ de polinômios em $\mathbb{K}[X_1, \ldots, X_n]$ definimos

$$V(\mathcal{F}) = \{a \in \mathbb{K}^n : f(a) = 0, \text{ para todo } f \in \mathcal{F}\}$$

o subconjunto de $\mathbb{K}^n$ que zera simultaneamente em todos os polinômios de $\mathcal{F}$. Dizemos que um conjunto $V \subset \mathbb{K}^n$ é *algébrico* se $V = V(\mathcal{F})$ para alguma família $\mathcal{F}$ de polinômios em $\mathbb{K}[X_1, \ldots, X_n]$.

Exemplo 1.1. A circunferência unitaria centrada na origem no $\mathbb{R}^2$ é um conjunto algébrico. De fato, considere o polinômio $f \in \mathbb{R}[x, y]$ dado por $f(x, y) = x^2 + y^2 - 1$. O conjunto dos seus zeros $V(f) = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ é exatamente a circunferência desejada.

Conjuntos algébricos são fechadas por união e interseção.

Proposição 1.2. *Se $V_1, V_2 \subset \mathbb{K}^n$ são dois conjuntos algébricos, então $V_1 \cap V_2$ e $V_1 \cup V_2$ também são algébricos.*

Demonstração. Se $V_1 = V(\mathcal{F}_1)$ e $V_2 = V(\mathcal{F}_2)$ para duas famílias de polinômios $\mathcal{F}_1$ e $\mathcal{F}_2$, então $V_1 \cap V_2 = V(\mathcal{F}_1 \cup \mathcal{F}_2)$ e $V_1 \cup V_2 = V(\mathcal{F}_1 \cdot \mathcal{F}_2)$ onde $\mathcal{F}_1 \cdot \mathcal{F}_2 = \{f_1 \cdot f_2 : f_1 \in \mathcal{F}_1, f_2 \in \mathcal{F}_2\}$. De fato,

$$a \in V(\mathcal{F}_1 \cup \mathcal{F}_2) \Leftrightarrow a \in V(\mathcal{F}_1) \cap V(\mathcal{F}_2) = V_1 \cap V_2$$

e

$$a \in V(\mathcal{F}_1 \cdot \mathcal{F}_2) \Leftrightarrow a \in V(\mathcal{F}_1) \cup V(\mathcal{F}_2) = V_1 \cap V_2.$$

A última afirmação segue da observação que se $a \notin V(\mathcal{F}_1)$, então existe $f_1 \in \mathcal{F}_1$ tal que $f_1(a) \neq 0$. Como $a \in V(\mathcal{F}_1 \cdot \mathcal{F}_2)$, então $f_1(a)g(a) = 0$ para todo $g \in \mathcal{F}_2$ e logo $a \in V(\mathcal{F}_2)$. □

Observação 1.3. Nem todo conjunto de $\mathbb{K}^n$ é um conjunto algébrico. Um exemplo é o conjunto $\mathbb{Z} \subset \mathbb{R}$. Se $\mathbb{Z} = V(\mathcal{F})$ para alguma família de polinômios em $\mathbb{R}[X]$ teriamos polinômios não nulos que zerariam em infinitos valores, o que contradiz o Teorema fundamental da álgebra.

Outro exemplo é o quadrado unitário $Q = [0,1]^2 \subset \mathbb{R}^2$. Se $f \in \mathbb{R}[x,y]$ é um polinômio não nulo tal que $f(Q) = 0$, então para todo $b \in [0,1]$, $f(x,b) = 0$ para todo $x \in [0,1]$. Porém $g_b(x) = f(x,b)$ é um polinômio em uma variável e pelo Teorema fundamental da álgebra tem de ser identicamente nulo, pois zera em todos os valores de $x \in [0,1]$. Assim segue que $g_b = 0$ para todo $b \in [0,1]$ o que contradiz f não ser nulo.

Dado um anel R dizemos que um subconjunto $I \subset R$ é um *ideal* se I satisfaz as seguintes propriedades:

1. Se $a, b \in I$, então $a + b \in I$.
2. Se $a \in I$ e $r \in R$, então $ra \in I$.

Na verdade, se o anel não for comutativo essa definição nos daria um ideal à direita (pois a multiplicação é feita pela direita). Porém como em todos os casos o nosso anel será comutativo não teremos problema. Dado um conjunto $A \in R$, o ideal $\langle A \rangle$ gerado por A é o ideal minimal contendo A, isto é, para todo I ideal com $A \subset I$, então $A \subset \langle A \rangle$. Uma outra forma de definir $\langle A \rangle$ é

$$\langle A \rangle = \{r_1 a_1 + \ldots + r_t a_t : a_i \in A, r_i \in R\}.$$

Proposição 1.4. *Seja R um anel comutativo com unidade. R é um corpo se, e somente se, os únicos ideais de R são $\{0\}$ e o próprio R.*

Demonstração. Suponha que R é um corpo. Seja I um ideal não vazio de R e $a \in I$. Do fato de R ser um corpo, existe $b \in R$ tal que $ab = 1$. Pela definição de ideal $1 = ba \in I$. Porém agora para todo $r \in R$, temos que $r \cdot 1 \in I$, ou seja, $I = R$.

Suponha que os únicos ideais de R sejam $\{0\}$ e R. Seja $r \in R$ um elemento do anel com $r \neq 0$. O ideal $\langle r \rangle$ é não vazio e portanto é igual a R. Mas $\langle r \rangle = \{ar : a \in R\}$ consiste exatamente dos múltiplos de r. Como $1 \in R$, segue que 1 é múltiplo de r, isto é, existe $s \in R$ tal que $rs = 1$. Isso implica que todo elemento não nulo de R possui inversa e logo R é um corpo. □

Uma observação interessante que podemos fazer sobre conjuntos algébricos até aqui é que dado uma família $\mathcal{F} \subset \mathbb{K}[X_1, \ldots, X_n]$ temos que $V(\mathcal{F}) = V(\langle \mathcal{F} \rangle)$. De fato, se $a \in V(\mathcal{F})$, então $f(a) = 0$ para todo $f \in \mathcal{F}$. Logo $(h_1 f_1 + \ldots + h_t f_t)(a) = 0$ para todos $f_1, \ldots, f_t \in \mathcal{F}$ e $h_1, \ldots, h_t \in \mathbb{K}[X_1, \ldots, X_n]$ e disso $a \in V(\mathcal{F})$, o que conclui que $V(\mathcal{F}) \subset V(\langle \mathcal{F} \rangle)$. O outro lado é imediato do fato de $\mathcal{F} \subset \langle \mathcal{F} \rangle$ e portanto $V(\langle \mathcal{F} \rangle) \subset V(\mathcal{F})$.

Isto tudo significa que o conjunto de zeros de uma família de polinômios se mantem ao considerarmos o ideal dessa família. Assim podemos supor sem perda de generalidade que $\mathcal{F}$ é sempre um ideal. Seria interessante se pudessemos gerar esse ideal com apenas um número finito de polinômios, o que facilitaria nosso entendimento desses conjuntos. Isso é possivel e se trata do Teorema da base de Hilbert.

Um anel R é *noetheriano* se toda sequência crescente de ideais estaciona, isto é, se para toda sequência $\{I_k\}_{k \in \mathbb{N}}$ de ideais em R tal que $I_1 \subset I_2 \subset \ldots \subset I_k \subset \ldots$ existe um $t \in \mathbb{N}$ tal que $I_t = I_{t+1} = I_{t+2} = \ldots$ Um ideal $I \subset R$ é finitamente gerado se existe um conjunto finito de elementos $\{a_1, \ldots, a_t\} \subset R$ tal que $I = \langle a_1, \ldots, a_t \rangle$.

Proposição 1.5. *R é noetheriano se, e somente se, todo ideal de R é finitamente gerado.*

Demonstração. Suponha que R é noetheriano. Seja I um ideal de R. Construa uma sequência de ideais $I_0, I_1, \ldots, I_k, \ldots$ da seguinte forma. Faça $I_0 = \{0\}$ e defina os próximos ideais recursivamente. Suponha que I_k já foi definido, se $I_k = I$, então faça $a_{k+1} = 0$ e $I_{k+1} = \langle a_{k+1} \rangle + I_k$. Caso contrário, seja $a_{k+1} \in I \setminus I_k$ um elemento qualquer, defina $I_{k+1} = \langle a_{k+1} \rangle + I_k$, isto é, o ideal gerado por I_k e a_{k+1}. Note que no último caso $I_k \subsetneq I_{k+1}$ e que para todo j, $I_j = \langle a_1, \ldots, a_j \rangle$.

Nos dois casos obtemos que a sequência $\{I_k\}_{k\in\mathbb{N}}$ é uma sequência crescente de ideais e que todos estão contidos em I. Como R é noetheriano, sabemos que essa sequência estaciona. Seja k o menor inteiro tal que $I_k = I_{k=1}$. A única forma de isso ocorrer é se $I = I_k = \langle a_1, \ldots, a_k\rangle$ e portanto I é finitamente gerado.

Suponha agora que todo ideal de R é finitamente gerado. Seja $I_0 \subset I_1 \subset \ldots \subset I_k \subset \ldots$ uma sequência crescente de ideais. Seja $I = \bigcup_{k=0}^{\infty} I_k$ a união desses ideais. Não é difícil ver que I também é um ideal. De fato, se $a, b \in I$, então existem I_l, I_m tais que $a \in I_l$, $b \in I_m$. Do fato da sequência ser crescente $a, b \in I_p$ onde $p = \max\{l, m\}$ e logo $a + b \in I_p \subset I$ e para todo $r \in R$ vale também que $ra \in I_p \subset I$.

Da hipótese temos que I é finitamente gerado. Suponha que $I = \langle a_1, \ldots, a_m\rangle$. Como $a_i \in I$ significa que existe $t_i \in \mathbb{N}$ tal que $a_i \in I_{t_i}$ para todo $1 \leq i \leq m$. Seja $t = \max\{t_1, \ldots, t_m\}$. Do fato dos ideais serem crescentes temos que $a_i \in I_t$ para todo $1 \leq i \leq m$. Logo $I = \langle a_1, \ldots, a_m\rangle \subset I_t \subset I$. Isso significa que $I_t = I_{t+1} = I_{t+2} = \ldots = I$, ou seja, a sequência estaciona. Portanto R é noetheriano. □

Teorema 1.6 (Base de Hilbert)**.** *Se R é noetheriano, então $R[X]$ é noetheriano.*

Demonstração. Seja I um ideal de $R[X]$, vamos mostrar que ele é finitamente gerado. Para isso vamos construir recursivamente uma sequência de ideais começando por $I_0 = \{0\}$. Dado I_k, construimos I_{k+1} da seguinte forma. Considere $f_{k+1} \in I \setminus I_k$ o polinômio de grau mínimo em $I \setminus I_k$, então $I_{k+1} = I_k + \langle f_{k+1}\rangle = \langle f_1, \ldots, f_{k+1}\rangle$. Se $I = I_k$ apenas pare.

Temos então duas possibilidades: Ou em algum momento essa sequência para e quando isso acontece temos um k tal que $I = I_k = \langle f_1, \ldots, f_k\rangle$ e logo I é finitamente gerado, ou $\{I_k\}_{k\in NN}$ é uma sequência infinita estritamente crescente. Nesse segundo caso, pela forma como foi construída temos que $\deg(f_1) \leq \deg(f_2) \leq \ldots \leq \deg(f_k) \leq \ldots$, ou seja, a sequência de graus dos polinômios f_i é crescente.

Para cada polinômio f_i seja a_i o coeficiente do termo lider de f_i. Defina a sequência $\{J_k\}_{k\in\mathbb{N}}$ de ideais em R dada por $J_k = \langle a_1, \ldots, a_k\rangle$. Essa sequência é obviamente crescente, e por R ser noetheriano existe m tal que a sequência estaciona. Em outras palavras, existe m tal que $\langle a_1, \ldots, a_m\rangle$ é o ideal gerado por $\{a_i\}_{i\in\mathbb{N}}$.

Vamos mostrar que $f_{m+1} \in \langle f_1, \ldots, f_m\rangle$ o que contradiz a forma como as funções f_i's foram escolhidas. Do fato de $a_{m+1} \in \langle a_1, \ldots, a_m\rangle$ existem $b_1, \ldots, b_m \in R$ tais que

$$a_{m+1} = \sum_{i=1}^{m} b_i a_i.$$

Então considere o polinômio $g \in I$ dado por

$$g = f_{m+1} - \sum_{i=1}^{m} b_i X^{\deg(f_{m+1})-\deg(f_i)} f_i.$$

Como o coeficiente lider de f_{m+1} é a_{m+1} e o de $\sum_{i=1}^{m} b_i X^{\deg(f_{m+1})-\deg(f_i)} f_i$ é $\sum_{i=1}^{m} b_i a_i$ temos que $\deg(g) < \deg(f_{m+1})$. Como f_{m+1} é o polinômio de menor grau em I fora do ideal $\langle f_1, \ldots, f_m\rangle$ segue que $g \in \langle f_1, \ldots, f_m\rangle$. Porém isso implica que $f_{m+1} \in \langle f_1, \ldots, f_m\rangle$, chegando na contradição desejada. □

No nosso caso em particular $\mathbb{K}$ é um corpo e pela Proposição 5.4 só possui como ideais $\{0\}$ e o próprio $\mathbb{K}$. Isso implica que $\mathbb{K}$ é noetheriano e logo pelo Teorema da Base de Hilbert, o anel $\mathbb{K}[X]$ é noetheriano. Agora notando que $\mathbb{K}[X_1, \ldots, X_n] = \mathbb{K}[X_1][X_2]\ldots[X_n]$, aplicações iteradas do Teorema 5.6 nos mostram que o anel $\mathbb{K}[X_1, \ldots, X_n]$ é noetheriano. Ou seja, todo ideal em $\mathbb{K}[X_1, \ldots, X_n]$ é gerado por um conjunto finito de polinômios.

Para finalizarmos vamos enunciar o Nullstellensatz Fraco. Vamos enunciar o teorema na forma de um teorema de alternativas. O que torna relativamente satisfatório do ponto de vista computacional.

Teorema 1.7 (Nullstellensatz Fraco)**.** *Dados $\mathbb{K}$ um corpo algebricamente fechado e polinômios $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$, então exatamente uma das alternativas vale:*

1. *Existe $a \in \mathbb{K}^n$ tal que $f_1(a) = \ldots = f_m(a) = 0$.*
2. *Existem $g_1, \ldots, g_m \in \mathbb{K}[X_1, \ldots, X_n]$ tais que $f_1 g_1 + \ldots + f_m g_m = 1$.*

◇ ◇ ◇ *Aula 2 (22 de Agosto) — Yoshiharu Kohayakawa* ◇ ◇ ◇

Uma outra maneira de enunciar o Nullstellensatz Fraco pode ser feita da seguinte forma.

Teorema 1.8 (Nullstellensatz Fraco). *Seja* $\mathbb{K}$ *um corpo algébricamente fechado e* I *um ideal em* $\mathbb{K}[X_1, \ldots, X_n]$. *Se* $V(I) = \varnothing$, *então* $I = \mathbb{K}[X_1, \ldots, X_n]$.

A equivalência com o Teorema 1.7 vem do teorema da base de Hilbert. Como $\mathbb{K}[X_1, \ldots, X_n]$ é noetheriano, segue que I é finitamente gerado. Escrevendo $I = \langle f_1, \ldots, f_m \rangle$, então $a \in V(I)$ se, e somente se $f_1(a) = \ldots = f_m(a) = 0$. Assim $V(I) = \varnothing$ significa que $f_1, \ldots, f_m$ não possuem uma raiz comum. A igualdade $I = \mathbb{K}[X_1, \ldots, X_n]$ ocorre se, e somente se $1 \in I$. Isso é fácil de ver. Se $1 \in I$ é obvio pela definição de ideal que $f = f \cdot 1 \in I$ para todo $f \in \mathbb{K}[X_1, \ldots, X_n]$, logo $I = K[X_1, \ldots, X_n]$. Agora se $I = K[X_1, \ldots, X_n]$, então todo polinômio $f \in I$. Em particular $1 \in I$.

Com essas observações, basicamente o Teorema 1.8 nos diz que se não existe uma raiz comum de $f_1, \ldots, f_m$, então existem $g_1, \ldots, g_m$ tais que $f_1 g_1 + \ldots + f_m g_m = 1$. Isso segue de imediato do Teorema 1.7. Já para vermos que o Teorema 1.7 segue de 1.8 basta ver que $f_1, \ldots, f_m$ possuirem uma raiz comum e $1 \in \langle f_1, \ldots, f_m \rangle$ não podem ocorrer simultaneamente. Se ocoressem, sendo $a \in \mathbb{K}^n$ raiz comum, então

$$1 = \sum_{i=1}^{m} (g_i f_i)(a) = 0$$

o que é uma contradição.

Observação 1.9. O Nullstellensatz Fraco necessita que $\mathbb{K}$ seja um corpo algebricamente fechado. Por exemplo, se $\mathbb{K} = \mathbb{R}$ que não é algebricamente fechado, um possível contra exemplo seria tomando $n = 1$ e o ideal $I = \langle X^2 + 1 \rangle$. Como $X^2 + 1$ não possui raízes em $\mathbb{R}$ temos que $V(I) = \varnothing$, porém $I \neq \mathbb{K}[X]$.

Outra observação é que no caso $n = 1$ o teorema pode ser facilmente provado notando que o anel $\mathbb{K}[X]$ é um domínio de ideais principais, isto é, todo ideal em $\mathbb{K}[X]$ é gerado por apenas um polinômio. Uma maneira de provar isso vem da divisão euclideana que está bem definido em $\mathbb{K}[X]$. O algoritmo da divisão euclideana nos garante que para polinômios $f, g \in \mathbb{K}[X]$ existem polinômios $q, r \in \mathbb{K}[X]$ tais que $g = fq + r$ e $deg(r) < deg(g)$.

Dado um ideal $I \in \mathbb{K}[X]$ seja f um polinômio não nulo de menor grau em I. Seja $g \in I$ um polinômio qualquer. Pela divisão euclideana $g = fq + r$ para $q, r \in \mathbb{K}[X]$ e $deg(r) < deg(f)$. Mas aí temos um problema: pela definição de ideal o polinômio r tem de pertencer a I, porém f é um polinômio de menor grau. A única forma de isso ocorrer é se $r = 0$ e neste caso $g = fq$, ou seja, g é múltiplo de f. Isso conclui que $I = \langle f \rangle$. Então se $V(I) = \varnothing$ temos que I tem de ser gerado por um polinômio f de grau 0, pois $\mathbb{K}$ é algebricamente fechado. Isso significa que $1 \in I$ e logo $I = \mathbb{K}[X]$.

Estudamos até agora ideais I no conjunto de polinômios $\mathbb{K}[X_1, \ldots, X_n]$ e conjuntos algébricos V em $\mathbb{K}^n$. Esses dois espaços possuem uma conexão simples como já vimos. Para cada ideal I, existe um conjunto algébrico $V(I)$ cujo os elementos são os zeros comuns dos polinômios em I e para cada conjunto algébrico V existe um ideal de polinômios $I(V)$ tal que V é o conjunto dos zeros comuns de $I(V)$. Podemos estender essas relações para o $\mathbb{K}^n$ e o $\mathbb{K}[X_1, \ldots, X_n]$.

Seja $I : \mathcal{P}(\mathbb{K}^n) \to \mathcal{I}$ uma função que leva um subconjunto de $\mathbb{K}^n$ em um ideal de $\mathbb{K}[X_1, \ldots, X_n]$ (denotamos por $\mathcal{I}$ o conjunto de ideais de $\mathbb{K}[X_1, \ldots, X_n]$). Dado um conjunto $S \subset \mathbb{K}^n$ definimos $I(S)$ como o menor ideal em $\mathbb{K}[X_1, \ldots, X_n]$ tal que para todo $f \in I(S)$, temos $f(S) = 0$. Como $0 \in I(S)$ para todo S, esse ideal sempre existe.

Da mesma forma podemos definir a aplicação $V : \mathcal{P}(\mathbb{K}[X_1, \ldots, X_n]) \to \mathcal{P}(\mathbb{K}^n)$ que leva conjuntos de polinômios em $\mathbb{K}[X_1, \ldots, X_n]$ em subconjuntos algébricos em $\mathbb{K}^n$. Dado um conjunto $\mathcal{F} \subset \mathbb{K}[X_1, \ldots, X_n]$ temos que $V(\mathcal{F})$ é o subconjunto de elementos de $\mathbb{K}^n$ que zeram em todos os polinômios de $\mathcal{F}$, como já definido previamente.

Considere a ordem parcial usual de inclusão nos conjuntos $\mathbb{K}^n$ e $\mathbb{K}[X_1, \ldots, X_n]$. As funções I e V agem nesses conjuntos invertendo ordens, em outras palavras, se $S_1 \subset S_2$, então $I(S_2) \subset I(S_1)$ e se $\mathcal{F}_1 \subset \mathcal{F}_2$, então $V(\mathcal{F}_2) \subset V(\mathcal{F}_1)$. Em geral, dado dois conjuntos parcialmente ordenados $(P_1, \leq_1)$ e $(P_2, \leq_2)$ dizemos que as duas funçoes $f : P_1 \to P_2$ e $g : P_2 \to P_1$ formam uma *conexão de Galois* entre P_1 e P_2 se elas invertem ordens, isto é, se $a \leq_1 b \Rightarrow f(b) \leq_2 f(a)$ para $a, b \in P_1$ e $a \leq_2 b \Rightarrow g(b) \leq_1 g(a)$ para $a, b \in P_2$, e se $a \leq_1 g(b) \Leftrightarrow b \leq_2 f(a)$ para $a \in P_1$ e $b \in P_2$. O nome vem do famoso resultado em teoria de Galois que extensões de corpos e grupos podem ser relacionados por funções como vistas acima. Apenas a definição de conexão de Galois já nos permite analisar o que acontece ao aplicarmos $f \circ g$ ou $g \circ f$.

Proposição 1.10. *Dado* $a \in P_1$ *e* $b \in P_2$, *temos que* $a \leq_1 g(f(a))$ *e* $b \leq_2 f(g(b))$.

Demonstração. Do fato de f e g formarem uma conexão de Galois temos que $a \leq_1 g(b) \Leftrightarrow b \leq_2 f(a)$. Tomando $a = g(b)$ obtemos que $b \leq_2 f(g(b))$ e tomando $b = f(a)$ obtemos que $a \leq_1 g(f(a))$. □

A última proposição pode ser aplicada no nosso caso, pois estamos lidando com uma conexão de Galois. De fato, já mostramos que I e V invertem ordem, basta provar que para $S \in \mathbb{K}^n$ e $\mathcal{F} \in \mathbb{K}[X_1, \ldots, X_n]$ temos que $S \subset V(\mathcal{F}) \Leftrightarrow \mathcal{F} \subset I(S)$. Isto é verdade pois as duas afirmações são equivalentes a dizer que para todo $f \in \mathcal{F}$ temos que $f|_S = 0$. Assim por I e V formarem uma conexão de Galois sobre $\mathbb{K}^n$ e $\mathbb{K}[X_1, \ldots, X_n]$ a Proposição 5.9 nos garante que para todo $S \in \mathbb{K}^n$ temos $S \subset V(I(S))$ e para todo $\mathcal{F} \in \mathbb{K}[X_1, \ldots, X_n]$ temos $\mathcal{F} \subset I(V(\mathcal{F}))$. Na verdade conseguimos algo um pouco melhor.

Proposição 1.11. *Se $S \in \mathbb{K}^n$ é um conjunto algébrico, então $S = V(I(S))$.*

Demonstração. Já mostramos que $S \subset V(I(S))$ para todo $S \in \mathbb{K}^n$. Resta mostra que se S é conjunto algébrico, então $V(I(S)) \subset S$. De fato, se S é conjunto algébrico, então $S = V(\mathcal{F})$ para algum conjunto de polinômios $\mathcal{F} \subset \mathbb{K}[X_1, \ldots, X_n]$. Usando da Proposição 5.9 temos que $\mathcal{F} \subset I(V(\mathcal{F}))$. Aplicando V dos dois lados e usando que V inverte ordem obtemos que

$$V(I(V(\mathcal{F}))) \subset V(\mathcal{F}) \Leftrightarrow V(I(S)) \subset S.$$

□

Nós poderiamos pensar que o análogo acontece do outro lado, isto é, se $\mathcal{F}$ é um ideal então $\mathcal{F} = I(V(\mathcal{F}))$. Porém isso não é verdade. Um contra exemplo é o ideal $\langle X_1^3 \rangle$. O conjunto algébrico $V(\langle X_1^3 \rangle)$ consiste de todos os elementos em $\mathbb{K}^n$ cuja primeira coordenada é 0. Disso é fácil ver que $X_1 \in I(V(\langle X_1^3 \rangle))$ porém $X_1 \notin \langle X_1^3 \rangle$.

Em vista dessa dificuldade técnica precisamos definir o radical de um ideal. Dado um anel R e um ideal I definimos o radical $rad(I)$ de I como

$$rad(I) = \{a \in R : a^s \in I \text{ para algum } s \in \mathbb{N}\}$$

O primeiro passo é checar que o radical de um ideal é também um ideal.

Proposição 1.12. *Dado um anel R e um ideal I o radical $rad(I)$ é um ideal em R.*

Demonstração. Sejam $a, b \in rad(I)$. Da definição existem s_1, s_2 tais que $a^{s_1}, b^{s_2} \in I$. Tome agora $s = s_1 + s_2$ e analisemos $(a+b)^s$. Expandindo pelo binômio de newton obtemos

$$(a+b)^s = \sum_{i=0}^{s} \binom{s}{i} a^i b^{s-i}.$$

Do fato de $s \geq s_1 + s_2$ temos que ou $i \geq s_1$ ou $s - i \geq s_2$, para todo $0 \leq i \leq s$. Isso significa que para todo $1 \leq i \leq s$ o monômio $a^i b^{s-1}$ pertence a I. Portanto $(a+b)^s \in I$ e consequentemente $a + b \in rad(I)$. Como $a^{s_1} \in I$ e I é um ideal, temos que $r^{s_1} a^{s_1} \in I$ para todo $r \in R$ e portanto $ra \in rad(I)$ para todo $r \in R$. Isso conclui que $rad(I)$ é um ideal. □

É obvio que $J \subset rad(J)$ para um ideal $J \subset \mathbb{K}[X_1, \ldots, X_n]$. O natural é perguntar se $rad(J)$ é o suficiente, isto é, $rad(J)$ é $I(V(J))$. Se $g \in rad(J)$, então $g^t \in J$ para algum $t \in \mathbb{N}$. Isso significa que $g^t|_{V(J)} = 0$, pela definição de $V(J)$ e como $\mathbb{K}$ é um corpo ele não possui divisores de zero e portanto $g|_{V(J)} = 0$. Mas o útlimo é exatamente o mesmo de dizer que $g \in I(V(J))$, logo $rad(J) \subset I(V(J))$. O Nullstellensatz nos garante que a outra inclusão também vale.

Teorema 1.13 (Nullstellensatz Forte)**.** *Seja $J = \langle f_1, \ldots, f_m \rangle$ um ideal em $\mathbb{K}[X_1, \ldots, X_n]$ gerado pelos polinômios $f_1, \ldots f_m$ e seja $V = V(J)$ o conjunto de zeros comuns a esses polinômios. Se para um polinômio $g \in \mathbb{K}[X_1, \ldots, X_n]$ temos $g|_V = 0$, então existem $t \in \mathbb{N}$ e $h_1, \ldots, h_m \in \mathbb{K}[X_1, \ldots, X_n]$ tais que*

$$g^t = h_1 f_1 + \ldots + h_m f_m.$$

Demonstração. Para provarmos o Nullstellensatz Forte vamos usar o Nullstellensatz Fraco. Seja Y uma nova variável e considere o anel $\mathbb{K}[X_1, \ldots, X_n, Y]$. Os polinômios $f_1, \ldots, f_m, g$ podem ser vistos

como elementos de $\mathbb{K}[X_1,\ldots,X_n,Y]$ pois utilizam um número menor de variáveis. Considere o polinômio $f_{m+1} \in \mathbb{K}[X_1,\ldots,X_n,Y]$ dado por $f_{m+1}(X_1,\ldots,X_n,Y) = Yg(X_1,\ldots,X_n) - 1$. Vamos mostrar que $f_1,\ldots,f_{m+1}$ não possuem uma raiz em comum.

Suponha que estes polinômios tenham uma raiz comum e seja $(a_1,\ldots,a_n,b)$ essa raiz. Como $f_1(a_1,\ldots,a_n) = \ldots = f_m(a_1,\ldots,a_n) = 0$ segue que $(a_1,\ldots,a_n) \in V(J)$ e logo $g(a_1,\ldots,a_n) = 0$ pela hipótese. Temos então que $f_{m+1}(a_1,\ldots,a_n,b) = bg(a_1,\ldots,a_n) - 1 = -1 \neq 0$, o que contradiz o fato de $(a_1,\ldots,a_n,b)$ ser uma raiz comum.

Pelo Teorema 1.7 existem $h_1,\ldots,h_{m+1} \in \mathbb{K}[X_1,\ldots,X_n,Y]$ tais que $h_1f_1 + \ldots + h_{m+1}f_{m+1} = 1$. Expandindo f_{m+1} temos

$$1 = \sum_{i=1}^{m} h_i(X_1,\ldots,X_n,Y)f_i(X_1,\ldots,X_n) + h_{m+1}(X_1,\ldots,X_n,Y)(Yg(X_1,\ldots,X_n) - 1).$$

Tomando $Y = \frac{1}{g(X_1,\ldots,X_n)}$ obtemos

$$1 = \sum_{i=1}^{m} h_i(X_1,\ldots,X_n,\frac{1}{g(X_1,\ldots,X_n)})f_i(X_1,\ldots,X_n).$$

Seja t um expoente grande suficiente tal que o expoente de Y em qualquer polinomio h_i seja menor que t, então multiplicando a última equação por g^t temos

$$g(X_1,\ldots,X_n)^t = \sum_{i=1}^{m} g(X_1,\ldots,X_n)^t h_i(X_1,\ldots,X_n,\frac{1}{g(X_1,\ldots,X_n)})f_i(X_1,\ldots,X_n) = \sum_{i=1}^{m} \tilde{h}_i(X_1,\ldots,X_n)f_i(X_1,\ldots,X_n).$$

porque podemos ver $g(X_1,\ldots,X_n)^t h_i(X_1,\ldots,X_n,\frac{1}{g(X_1,\ldots,X_n)})$ como um polinômio em $X_1,\ldots,X_n$ pela escolha de t. □

◇ ◇ ◇ *Aula 3 (12 de Setembro) — Yoshiharu Kohayakawa* ◇ ◇ ◇

Nessa aula provaremos o Nullstellensatz Fraco (Teoremas 1.7 e 1.8). Faremos isso por indução no número de indeterminadas. O caso $n = 1$ já foi estudado na Observação 1.9. Lá mostramos que o algoritmo da divisão euclideana era essencial para mostrar que qualquer ideal I em $\mathbb{K}[X]$ podia ser gerado por um único elemento. Esse gerador do ideal I é um divisor comum de todos os elementos de I, mas mais do que isso, é o máximo divisor comum de todos os elementos de I.

Uma maneira muito natural de conseguir esse gerador vem pelo Teorema de Bezout, em que dados dois polinômios $f,g \in \mathbb{K}[X]$ nós encontramos polinômios $a,b \in \mathbb{K}[X]$ com $deg(a) < deg(g) - 1$ e $deg(b) < deg(f) - 1$ tais que o máximo divisor em comum mônico $h \in \mathbb{K}[X]$ pode ser expresso como $h = af + bg$. Para os nossos propósitos vamos precisar de uma forma eficiente de calcular esse máximo divisor comum em um contexto um pouco mais geral.

Seja R um anel noetheriano de domínio integral, i.e., se $a,b \in R$ sao tais que $ab = 0$ então ou $a = 0$, ou $b = 0$. Dados dois polinômios $f,g \in R[X]$ não nulos de graus n,m, respectivamente, com

$$f(X) = f_0 + f_1X + \ldots + f_nX^n$$
$$g(X) = g_0 + g_1X + \ldots + g_mX^m$$

nós definimos o resultante de f,g como o determinante da matriz $(n+m)\times(n+m)$, $M_{f,g}$ dada por

$$M_{f,g} = \begin{pmatrix} f_0 & 0 & \cdots & 0 & g_0 & 0 & \cdots & 0 \\ f_1 & f_0 & \cdots & 0 & g_1 & g_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ f_n & f_{n-1} & \ddots & f_0 & g_m & g_{m-1} & \ddots & g_0 \\ 0 & f_n & \ddots & \vdots & 0 & g_m & \ddots & \vdots \\ \vdots & \vdots & \ddots & f_n & \vdots & \vdots & \ddots & g_m \end{pmatrix}.$$

Mais formalmente podemos definir $M_{f,g} = (m_{ij}) \in R^{(n+m)\times(n+m)}$ como

$$m_{ij} = \begin{cases} f_k, & \text{se } i-j=k \text{ e } j \le m \\ g_k, & \text{se } i-j-m=k \text{ e } j > m \\ 0, & \text{caso contrário} \end{cases}.$$

A matriz $M_{f,g}$ é interessante pois podemos expressar qualquer combinação da forma $af+bg$ com $deg(a) < deg(g)$ e $deg(b) < deg(f)$ como uma transformação linear. De fato, considere $a(X) = a_0 + a_1X + \ldots + a_{m-1}X^{m-1}$ e $b(X) = b_0 + b_1X + \ldots + b_{n-1}X^{n-1}$. Então se considerarmos $v \in R^{n+m}$ o vetor cuja entradas são

$$v_i = \begin{cases} a_{i-1}, & \text{se } i \le m \\ b_{i-m-1}, & \text{se } i > m \end{cases},$$

temos que uma simples conta nos mostra que $a(X)f(X) + b(X)g(X) = u_1 + u_2X + \ldots + u_{m+n}X^{n+m}$ onde $u = M_{f,g}v$. Em particular, o problema de saber se existe determinado polinômio h de grau no máximo $n+m-1$ tal que $h = af+bg$ é equivalente a saber se um sistema de equações da forma $M_{f,g}v = u$ possui solução. Isso depende fortemente do valor do determinante de $M_{f,g}$. De fato, no caso em que R é um corpo, o sistema acima possui solução se o determinante for diferente de 0. Para um anel R mais geral nós temos.

Lema 1.14. *O resultante $R_{f,g} = det(M_{f,g})$ é um elemento do ideal gerado por f, g em $R[X]$.*

Demonstração. O determinante é uma aplicação multilinear alternada, portanto isso nos permite somar a uma linha combinações lineares de outras linhas da matriz sem alterar o valor do determinante. Tendo isso em vista, chame m_i a i-ésima linha de $M_{f,g}$. Substitua m_1 por $m_1 + Xm_2 + \ldots + X^{n+m-1}m_{n+m}$. A nova matriz A obtida por essa substituição possui primeira linha com coordenadas $f(X), Xf(X), \ldots, X^{m-1}f(X), g(X), \ldots, X^{n-1}g(X)$. Calculando o determinante nós obtemos

$$R_{f,g} = det(A) = p(X)f(X) + q(X)g(X)$$

para polinômios $p, q \in R[X]$. Portanto $R_{f,g} \in \langle f, g \rangle$. □

Como todas as entradas de $M_{f,g}$ pertencem a R, uma consequência do último lema é que se $R_{f,g} \neq 0$, então f e g não possuem um fator não constante em comum. Em particular, se f e g possuem uma raiz em comum, então $R_{f,g} = 0$. O próximo lema é muito importante para nossa demonstração e é um caso particular do que é chamado de Lema de normalização de Noether.

Lema 1.15. *Seja $\mathbb{K}$ um corpo infinito e $f \in \mathbb{K}[X_1, \ldots, X_n]$ um polinômio de grau d. Então existem $\lambda_1, \ldots, \lambda_{n-1}$ tais que*

$$[X_n^d]f(X_1 + \lambda_1X_n, \ldots, X_{n-1} + \lambda_{n-1}X_n, X_n) \neq 0.$$

Demonstração. Observe que o polinômio $g(X_1, \ldots, X_n) = f(X_1 + \lambda_1X_n, \ldots, X_{n-1} + \lambda_{n-1}X_n, X_n)$ possui grau d e portanto o coeficiente de X_n^d em g vem do termo homogêneo de grau d de f. Isto é, se escrevermos $f = f_d + h$ onde f_d é o polinômio homogeneo de grau d de f, então uma simples conta nos mostra que $[X_n^d]g(X_1, \ldots, X_n) = [X_n^d]f_d(X_1 + \lambda_1X_n, \ldots, X_{n-1} + \lambda_{n-1}X_{n-1}, X_n) = f_d(\lambda_1, \ldots, \lambda_{n-1}, 1)$. Assim basta mostrarmos que existem $\lambda_1, \ldots, \lambda_{n-1}$ em $\mathbb{K}$ tais que o polinômio $p(X_1, \ldots, X_{n-1}) = f_d(X_1, \ldots, X_{n-1}, 1)$ de $(n-1)$ variáveis e grau no máximo d satisfaz $p(\lambda_1, \ldots, \lambda_{n-1}) \neq 0$.

Vamos mostrar por indução que isso ocorre para todo polinômio não nulo $p \in \mathbb{K}[X_1, \ldots, X_k]$. Se $k = 1$, então pelo teorema fundamental da álgebra existem apenas um número finito de raizes para p. Como $\mathbb{K}$ é infinito, existe λ tal que $p(\lambda) \neq 0$. Agora suponha que já provamos para $k-1$ indeterminadas, vamos provar para $p \in \mathbb{K}[X_1, \ldots, X_k]$. Podemos ver p como um polinômio em X_k. De fato, seja $q \in R[X_k]$ onde $R = \mathbb{K}[X_1, \ldots, X_{k-1}]$ e $q(X_k) = \sum_{i=0}^{t} q_i(X_1, \ldots, X_{k-1})X_k^i = p(X_1, \ldots, X_k)$. Por hipótese de indução seja $(\lambda_1, \ldots, \lambda_{k-1}) \in \mathbb{K}^{k-1}$ tal que $q_0(\lambda_1, \ldots, \lambda_{k-1}) \neq 0$. Se existe $a \in \mathbb{K}$ tal que $q(a) \neq 0$ então $p(\lambda_1, \ldots, \lambda_{k-1}, a) \neq 0$ e estamos resolvidos. Caso contrário, para todo $a \in \mathbb{K}$ temos que $q(a) = 0$ e logo do fato de $\mathbb{K}$ ser infinito temos que $q_i(\lambda_1, \ldots, \lambda_{k-1}) = 0$ para todo $i = 0, \ldots, t$. Em particular $q_0(\lambda_1, \ldots, \lambda_{k-1}) = 0$ o que é um absurdo.

□

O Lema 1.15 é verdadeiro apenas para corpos infinitos. Este é o nosso caso, pois todo corpo algebricamente fechado tem de ser infinito. De fato, suponha que $\mathbb{K}$ é um corpo algebricamente fechado. Considere o polinômio $f(X) = \prod_{a\in\mathbb{K}}(X-a)+1$. É fácil ver que $f(a) = 1$ para todo $a \in \mathbb{K}$ o que implica que f não possui raizes, uma contradição ao fato de $\mathbb{K}$ ser algebricamente fechado. Então nosso corpo satisfaz as condições do lema. Assim podemos provar o Teorema 1.8.

Demonstração do Teorema 1.8. A demonstração será por indução em n. O caso $n = 1$ já foi observado. Suponha agora que para todo $k < n$ o teorema é verdadeiro, vamos provar para n. Seja I um ideal de $\mathbb{K}[X_1,\ldots,X_n]$ que não contém 1 e suponha que exista $f \in I$ de grau d com

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

tal que $f_d \in \mathbb{K}^*$ e $f_i \in \mathbb{K}[X_1,\ldots,X_{n-1}]$.

Defina J como o ideal formado por todos os polinômios em I que não utilizam a indeterminada X_n, isto é, $J = I \cap \mathbb{K}[X_1,\ldots,X_{n-1}]$. É fácil ver que $1 \notin J$, pois $1 \notin I$. Como J pode ser visto como um ideal de $\mathbb{K}[X_1,\ldots,X_{n-1}]$ por hipótese de indução temos que $V(J) \neq \varnothing$. Seja $a = (a_1,\ldots,a_{n-1}) \in V(J)$ uma raíz comum a todos os elementos de J. Considere agora o ideal em $\mathbb{K}[X]$ dado por

$$I_a = \{f(a_1,\ldots,a_{n-1},X) : f \in I\} \subset \mathbb{K}[X].$$

Se $1 \notin I_a$, então pela hipótese de indução para o caso $n = 1$ temos que existe $V(I_a) \neq \varnothing$. Seja $a_n \in V(I_a$, é fácil ver que $(a_1,\ldots,a_n) \in V(I)$ e terminamos.

Assim basta mostrar que $1 \notin I_a$. Suponha que não, então existe $g \in I$ tal que $g(a_1,\ldots,a_{n-1},X_n) = 1$. Escreva

$$g(X_1,\ldots,X_n) = g_e(X_1,\ldots,X_{n-1})X_n^e + \ldots + g_1(X_1,\ldots,X_{n-1})X_n + g_0(X_1,\ldots,X_{n-1}).$$

Se $e > d$ então considere $f := X_n^{e-f}f$, caso contrário podemos ver g como um polinômio de grau d em X_n em que vale $g_i(X_1,\ldots,X_{n-1}) = 0$ para $i > e$. Seja $l = \max\{d,e\}$. Calcularemos o resultante $R_{g,f}$ como o determinante da matriz $2l \times 2l$ $M_{g,f}$ onde o anel é $R = \mathbb{K}[X_1,\ldots,X_{n-1}]$.

O Lema 1.14 nos diz que $R_{g,f} \in \langle f,g\rangle \subset I$, mas pela definição de resultante temos também que $R_{g,f} \in \mathbb{K}[X_1,\ldots,X_{n-1}$. Assim $R_{g,f} \in J$ e logo $R_{g,f}(a_1,\ldots,a_{n-1}) = 0$. Porém para esses valor temos que $g_0(a_1,\ldots,a_{n-1}) = 1$ e $g_i(a_1,\ldots,a_{n-1}) = 0$ para todo $i > 0$. Logo calculando explicitamente temos

$$R_{g,f}(a_1,\ldots,a_n) = det\begin{vmatrix} 1 & 0 & \cdots & 0 & f_0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & f_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & f_{l-1} & \cdots & f_0 \\ 0 & 0 & \cdots & 0 & f_l & \cdots & f_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & f_l \end{vmatrix} = f_l^l \neq 0$$

pois $f_l = f_d \neq 0$, uma contradição.

Agora suponha que I não possui um polinômio f como o de cima. Seja h um polinômio qualquer de I de grau d. O Lema 1.15 nos diz que existem $\lambda_1,\ldots,\lambda_{n-1}$ tais que

$$[X_n^d]h(X_1+\lambda_1X_n,\ldots,X_{n-1}+\lambda_{n-1}X_n,X_n) \neq 0.$$

Considere a aplicação $\phi : I \to \phi(I)$ que leva o ideal I em um ideal I' pela relação

$$\phi(f)(X_1,\ldots,X_n) = f(X_1+\lambda_1X_n,\ldots,X_{n-1}+\lambda_{n-1}X_n,X_n).$$

Não é difícil ver que ϕ é um isomorfismo. Porém $\phi(h)$ é um polinômio cujo coeficiente de X_n^d é não nulo. Isso significa que o teorema é verdadeiro para o ideal $\phi(I)$. Portanto existe $(b_1,\ldots,b_n) \in V(\phi(I))$. Aplicando a inversa notamos que $(b_1-\lambda_1b_n,\ldots,b_{n-1}-\lambda_{n-1}b_n,b_n)$ é uma raiz comum de I e logo $V(I) \neq \varnothing$.

□

◇ ◇ ◇ *Aula 4 (19 de Setembro) — Yoshiharu Kohayakawa* ◇ ◇ ◇

Agora trabalharemos com uma versão específica do Nullstellensatz. Como vimos nas aulas passadas o Nullstellensatz Forte nos diz que se $\mathbb{K}$ é um corpo algebricamente fechado e $g, f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$ são polinômios em n variáveis tais que $g \mid_{V(\{f_1,\ldots,f_m\})} = 0$, então existe inteiro t e polinômios $h_1, \ldots, h_m \in \mathbb{K}[X_1, \ldots, X_n]$ tais que

$$g^t = h_1 f_1 + \ldots + h_m f_m.$$

Façamos um caso particular em que $m = n$. Dados conjuntos finitos $S_1, \ldots, S_n$ em $\mathbb{K}$ defina $f_i = \prod_{s \in S_i}(X_i - s) \in \mathbb{K}[X_1, \ldots, X_n]$ para todo $1 \leq i \leq n$. Seja $g \in \mathbb{K}[X_1, \ldots, X_n]$ tal que $g(s_1, \ldots, s_n) = 0$ para todo $(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$. O Teorema 1.13 nos garante que existe um inteiro t e polinômios $h_1, \ldots, h_n$ tais que $g^t = f_1 h_1 + \ldots + f_n h_n$. Porém aqui conseguimos provar algo ainda mais forte.

Teorema 1.16. *Seja $\mathbb{K}$ um corpo qualquer e n um inteiro. Dados conjuntos finitos $S_1, \ldots, S_n$ em $\mathbb{K}$ podemos definir $f_i = \prod_{s \in S_i}(X_i - s) \in \mathbb{K}[X_1, \ldots, X_n]$. Seja $g \in \mathbb{K}[X_1, \ldots, X_n]$ tal que $g \mid_{S_1 \times \ldots \times S_n} = 0$. Então existem polinômios $h_1, \ldots, h_n$ com $deg(h_i) \leq deg(g) - deg(f_i)$ tais que*

$$g = h_1 f_1 + \ldots + h_n f_n.$$

Além disso, se os coeficientes de $g, f_1, \ldots, f_n$ pertencem a um anel $R \subset \mathbb{K}$, então os coeficientes de $h_1, \ldots, h_n$ também pertencem a esse anel.

O Teorema 1.16 possui diversas melhorias comparado ao Teorema 1.13. Melhorias como: podemos tomar $t = 1$, temos um maior controle do grau dos polinômios e acima de tudo $\mathbb{K}$ não precisa ser algebricamente fechado. Esse último ponto é de extrema importância em combinatória, onde os corpos naturais costumam ser finitos.

Para provarmos o teorema vamos precisar de um lema muito semelhante a demonstração do Lema 1.15.

Lema 1.17. *Seja $\mathbb{K}$ um corpo qualquer e $p \in \mathbb{K}[X_1, \ldots, X_n]$ um polinômio de n variáveis. Suponha para todo $1 \leq i \leq n$ que t_i é o maior expoente da variável X_i em todos os monômios de p e que $S_i \subset \mathbb{K}$ é um conjunto com $t_i + 1$ elementos. Se $p \mid_{S_1 \times \ldots \times S_n} = 0$, então p é o polinômio identicamente nulo.*

Demonstração. Faremos por indução em n. Se $n = 1$ isso é exatamente o fato que um polinômio não nulo de uma variável de grau t só pode ter t raízes (Teorema fundamental da Álgebra). Agora suponha por indução que o Lema é verdadeiro para $n - 1$ variáveis e vamos provar para n. Escreva p como

$$p = p_{t_n} X_n^{t_n} + \ldots + p_1 X_n + p_0$$

onde $p_i \in \mathbb{K}[X_1, \ldots, X_{n-1}]$. Fixe $(s_1, \ldots, s_{n-1}) \in S_1 \times \ldots \times S_{n-1}$, o polinômio

$$q(X) = p(s_1, \ldots, s_{n-1}, X) = p_{t_n}(s_1, \ldots, s_{n-1}) X^{t_n} + \ldots + p_1(s_1, \ldots, s_{n-1}) X + p_0(s_1, \ldots, s_{n-1})$$

de uma variável zera em todos os valores de S_n. Como $|S_n| > t_n$ isso significa que q tem de ser identicamente nulo, isto é, $p_i(s_1, \ldots, s_{n-1}) = 0$ para todo $1 \leq i \leq n$. Porém $(s_1, \ldots, s_{n-1})$ foi escolhido arbitrariamente, isso significa que $p_i(x_1, \ldots, x_{n-1}) = 0$ para todo $(x_1, \ldots, x_{n-1}) \in S_1 \times \ldots \times S_{n-1}$ e $1 \leq i \leq n$. Por hipótese de indução segue que todos os p_i's são identicamente nulos e logo p também é. □

Podemos agora demonstrar o teorema 1.16.

Demonstração do Teorema 1.16. Seja $t_i = |S_i| - 1$ para todo $1 \leq i \leq n$. Podemos então reescrever os polinômios f_i como

$$f_i(X_1, \ldots, X_n) = X_i^{t_i+1} - \sum_{j=0}^{t_i} f_{ij} X_i^j.$$

Como f_i será sempre que X_i assume um valor em S_i, isso significa que para $s \in S_i$ temos

$$s^{t_i+1} = \sum_{j=0}^{t_i} f_{ij} s^j.$$

Agora considere g como um polinômio em X_i, isto é, podemos escrever $g = g_d X_i^d + \ldots + g_1 X_i + g_0$ onde cada $g_j \in \mathbb{K}[X_1, \ldots, \widehat{X_i}, \ldots, X_n]$. Se $d > t_i$ podemos transformar esse polinômio em um polinômio de grau no máximo t_i substituindo X_i^l por $\sum_{j=l-t_i-1}^{l-1} f_{ij} X_i^j$ iteradamente até todos os monômios com X_i possuirem grau no máximo t_i. Isso pode ser feito subtraindo um polinômio da forma $h_i f_i$. Para exemplificar façamos uma iteração com o monômio $cX_1^{a_1} \ldots X_i^{a_i} \ldots X_n^{a_n}$

$$cX_1^{a_1} \ldots X_{i-1}^{a_{i-1}} \Big(\sum_{j=a_i-t_i-1}^{a_i-1} f_{ij} X_i^j \Big) X_{i+1}^{a_{i+1}} \ldots X_n^{a_n} = cX_1^{a_1} \ldots X_i^{a_i} \ldots X_n^{a_n} - cX_1^{a_1} \ldots \widehat{X_i}^{a_i} \ldots X_n^{a_n} f_i(X_1, \ldots, X_n).$$

Ou seja, para substituirmos $X_i^{a_i}$ precisamos subtrair algo da forma af_i com $a \in \mathbb{K}[X_1, \ldots, X_n]$. Aplicações iteradas dessa substituição nos dá o polinômio h_i. Note que da forma que o processo é feito $deg(h_i) \leq deg(g) - deg(f_i)$.

Fazendo isso para todo $1 \leq i \leq n$ obtemos polinômios $h_1, \ldots, h_n \in \mathbb{K}[X_1, \ldots, X_n]$ como no enunciado tais que $g - h_1 f_1 - \ldots - h_n f_n$ possui os expoentes de X_i menores ou iguais a t_i para todo $1 \leq i \leq n$. Como $(g - h_1 f_1 - \ldots - h_n f_n)(s_1, \ldots, s_n) = 0$ para todo $(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$ e $|S_i| = t_i + 1$ segue pelo Lema 1.17 que $g = h_1 f_1 + \ldots + h_n f_n$. Por fim, note que durante o processo de substituições os coeficientes de h_i são combinações lineares dos coeficientes de $g, f_1, \ldots, f_n$ e portanto pertencem ao mesmo subanel que esses coeficientes. □

Para aplicações combinatórias normalmente utilizamos o próximo teorema que é um corolário do último.

Teorema 1.18. *Seja $\mathbb{K}$ um corpo qualquer e $g \in \mathbb{K}[X_1, \ldots, X_n]$. Suponha que $deg(g) = \sum_{i=1}^n t_i$, onde cada t_i é um inteiro não negativo e suponha que o coeficiente de $\prod_{i=1}^n X_i^{t_i}$ em g é não nulo. Se $S_1, \ldots, S_n$ são subconjuntos de $\mathbb{K}$ com $|S_i| > t_i$, então existe $(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$ tal que $g(s_1, \ldots, s_n) \neq 0$.*

Demonstração. Suponha que não exista $(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$ tal que $g(s_1, \ldots, s_n) = 0$, isto é, suponha que $g|_{S_1 \times \ldots \times S_n} = 0$. Então se definirmos $f_i = \prod_{s \in S_i} (X_i - s)$ para todo $1 \leq i \leq n$ o Teorema 1.16 nos garante que existem $h_1, \ldots, h_n \in \mathbb{K}[X_1, \ldots, X_n]$ tais que $g = h_1 f_1 + \ldots + h_n f_n$. Agora vamos estudar cada termo da forma $h_i f_i$ separadamente. Como $deg(g) = \sum_{i=1}^n t_i$ então o monômio $\prod_{i=1}^n X_i^{t_i}$ tem o mesmo grau de g, isso significa que se ele aparecesse em $h_i f_i$ ele aparaceria como o monômio de maior grau. Porém para obtermos o monômio de maior grau temos que escolher o termo de maior grau em f_i que é $X_i^{|S_i|}$ cujo expoente é maior que t_i. Logo $\prod_{i=1}^n X_i^{t_i}$ não aparece em $h_i f_i$. Fazendo isso para todo i temos que o coeficiente de $\prod_{i=1}^n X_i^{t_i}$ em g é 0, o que é uma contradição. □

Teoremas 1.16 e 1.18 em conjunto são chamados de Nullstellensatz Combinatório. Vamos ver agora uma aplicação desses teoremas em um problema de combinatória aditiva. Seja $\mathbb{K} = \mathbb{F}_p$ o corpo finito de tamanho p, onde p é um primo. Dados dois conjuntos $A, B \subset \mathbb{F}_p$ podemos definir $A + B$ como

$$A + B = \{a + b : a \in A, b \in B\}.$$

Um problema central em combinatória aditiva é estimar o tamanho de $A + B$ para diversos grupos onde A, B estão definidos.

Para $\mathbb{F}_p$ podemos achar dois conjuntos A e B tais que $|A + B| = |A| + |B| - 1$ desde que $|A| + |B| - 1 \leq p$. De fato, escolha $A = \{1, \ldots, a\}$ e $B = \{1, \ldots, b\}$. Portanto $A + B = \{1, \ldots, a + b\}$ e logo $|A + B| = a + b - 1 = |A| + |B| - 1$. Se $a + b - 1 > p$, então nosso exmplo apenas dá $A + B = \mathbb{F}_P$ e $|A + B| = p$. Poderíamos nos perguntar se esse exemplo é o que gera $A + B$ de menor cardinalidade possível. Isso é verdade e é o Teorema de Cauchy-Davenport.

Teorema 1.19 (Cauchy-Davenport)**.** *Se p é um primo e A, B são dois subconjuntos não vazios de $\mathbb{F}_p$, então*

$$|A + B| \geq \min\{|A| + |B| - 1, p\}.$$

Demonstração. Vamos demonstrar o teorema utilizando do Nullstellensatz Combinatório. Se $|A|+|B|-1 \geq p$, então para qualquer $c \in \mathbb{F}_p$ temos que $(c-A)\cap B \neq \varnothing$, pois $|c-A|+|B| = |A|+|B| \geq p+1$ e pelo princípio da casa dos pombos estes dois conjuntos tem de possuir um element comum. Isso significa que existem $a \in A$ e $b \in B$ tais que $c = a+b \in A+B$ e logo $A+B = \mathbb{F}_p$. Assim podemos supor que $|A|+|B|-1 < p$.

Suponha agora que $|A+B| \leq |A|+|B|-2 < p$ e seja C um subconjunto de $\mathbb{F}_p$ tal que $A+B \subset C$ e $|C| = |A|+|B|-2$. Considere o polinômio $g \in \mathbb{F}_p[x,y]$ dado por

$$g(x,y) = \prod_{c\in C}(x+y-c).$$

O polinômio g possui grau $|A|+|B|-2$. Pela definição de C é fácil ver que $g\,|_{A\times B} = 0$. Assim do Nullstellensatz Combinatório temos que o coeficiente de $x^{|A|-1}y^{|B|-1}$ é 0, pois caso contrário teríamos que existe $(a,b) \in A\times B$ com $g(a,b) \neq 0$. Mas podemos calcular esse coeficiente

$$[x^{|A|-1}y^{|B|-1}]g(x,y) = \binom{|A|+|B|-2}{|A|-1} \neq 0$$

pois todos os termos no coeficiente binomial são menores que p e $\mathbb{F}_p$ não possui divisores de zero. Temos então uma contradição e o teorema está provado. □

2 Aplicações do Nullstellensatz Combinatório

◇ ◇ ◇ *Aula 5 (03 de Outubro) — Lucas Colucci* ◇ ◇ ◇

Agora veremos outras aplicações do Nullstellensatz Combinatório. Começaremos com uma aplicação em um problema de particionar elementos de um corpo finito.

Teorema 2.1. *Seja p um primo ímpar e $m = \frac{p-1}{2}$. Dado m elementos $d_1,\dots,d_m \in \mathbb{F}_p^*$, existem elementos $a_1,\dots,a_m,b_1,\dots,b_m \in \mathbb{F}_p^*$ distintos tais que*

$$b_i - a_i = d_i, \quad \forall\ 1 \leq i \leq m.$$

Basicamente o teorema anterior nos diz que podemos particionar os elementos de $\mathbb{F}_p^*$ em dois conjuntos $A = \{a_1,\dots,a_m\}$ e $B = \{b_1,\dots,b_m\}$ (pois $|\mathbb{F}_p^*| = p-1 = 2m$) com $b_i - a_i$ pré determinado. Em particular, se todos os $d_i = d$, Teorema 2.1 nos diz que existe um conjunto $A \subset \mathbb{F}_p^*$ tal que $A\cap(A+d) = \varnothing$ e $\mathbb{F}_p^* = A\cup(A+d)$.

A demonstração do teorema fará uso da forma do Nullstellensatz presente no Teorema 1.18. Para isso precisamos ser aptos a calcular o coeficiente de determinados monômios. O próximo lema nos permite fazer esse cálculo.

Lema 2.2. *(Conjectura de Dyson) Dados $a_1,\dots,a_n$ naturais. O coeficiente do termo livre de*

$$\prod_{1\leq i\neq j\leq n}(1-\frac{x_i}{x_j})^{a_i}$$

é $\binom{a_1+\dots+a_n}{a_1,\dots,a_n} = \frac{(a_1+\dots+a_n)!}{a_1!\dots a_n!}$.

Demonstração. Faremos a demonstração por indução em n e em $a_1+\dots+a_n$. Seja $f_n(a_1,\dots,a_n)$ o coeficiente do termo livre de $\prod_{1\leq i\neq j\leq n}(1-\frac{x_i}{x_j})^{a_i}$. Queremos mostrar que $f_n(a_1,\dots,a_n) = \frac{(a_1+\dots+a_n)!}{a_1!\dots a_n!}$. Vamos fazer isso em duas etapas.

Primeiro vamos mostrar que se algum dos $a_i's$ é zero, então podemos reduzir para o caso $n-1$. De fato, suponha sem perda de generalidade que $a_n = 0$. Então é fácil ver que

$$\prod_{1\leq i\neq j\leq n}(1-\frac{x_i}{x_j})^{a_i} = \prod_{\substack{1\leq i\neq j\leq n\\ i\neq n}}(1-\frac{x_i}{x_j})^{a_i}$$

e como não existem termos x_n no numerador, também não podemos ter termos x_n no denominador.

Isso significa que os únicos fatores da forma $(1-\frac{x_i}{x_j})^{a_i}$ que contribuem para o termo livre são os que $x_j \neq x_n$. Disso o coeficiente é o mesmo que o de

$$\prod_{1\leq i\neq j\leq n-1}(1-\frac{x_i}{x_j})^{a_i}$$

que é $f_{n-1}(a_1,\ldots,a_{n-1})$.

A segunda parte é mostrar que vale a seguinte recorrência

$$f_n(a_1,\ldots,a_n)=\sum_{i=1}^{n} f_n(a_1,\ldots,a_i-1,\ldots,a_n).$$

Para isso vamos precisar do polinômio interpolador de Lagrange. Suponha que $\prod_{1\leq i\neq j\leq n}(1-\frac{x_i}{x_j})^{a_i}$ é um elemento do corpo $\mathbb{K}=\mathbb{F}(x_1,\ldots,x_n)$. Seja $p\in\mathbb{K}[x]$ um polinômio de coeficientes em $\mathbb{K}$ tal que $deg(p)=n-1$ e $p(x_i)=1$ para todo $1\leq i\leq n$. O polinômio $g(x)=p(x)-1$ tem grau $n-1$ e é nulo para n valores. Pelo Teorema fundamental da Álgebra nós temos que $g\equiv 0$ e logo $p\equiv 1$. Porém podemos calcular usando o interpolador de Lagrange um polinômio p tal que $p(x_i)=1$ para todo $1\leq i\leq n$. De fato,

$$p(x)=\sum_{k=1}^{n}\prod_{j\neq k}\frac{(x_j-x)}{(x_j-x_k)}.$$

Para $x=0$ obtemos a igualdade

$$1=p(0)=\sum_{k=1}^{n}\prod_{j\neq k}\frac{x_j}{x_j-x_k}=\sum_{k=1}^{n}\prod_{j\neq k}(1-\frac{x_k}{x_j})^{-1}.$$

Multiplicando dos dois lados a nossa expressão original obtemos que

$$\prod_{1\leq i\neq j\leq n}(1-\frac{x_i}{x_j})^{a_i}=\sum_{k=1}^{n}\Big(\prod_{1\leq j\leq n}(1-\frac{x_k}{x_j})^{a_k-1}\prod_{\substack{1\leq i\neq j\leq n\\ i\neq k}}(1-\frac{x_i}{x_j})^{a_i}\Big).$$

O que significa que os coeficientes dos termos livres satisfazem a recursão desejada.

Agora só precisamos garantir que a base e o passo da indução estejam corretos. A base simplesmente consiste de um caso específico quando $n=2$. Se $n>1$ diversas iterações da recorrência nos garantirão que em algum momento um dos termos seja o, assim podemos diminuir o grau de n. Fazendo isso um número finito de vezes chegamos no caso em que $n=2$ e queremos calcular $f_2(a,0)$ ou $f_2(0,a)$. É fácil ver que em ambos os casos $f_2(a,0)=f_2(0,a)=1=\frac{(a+0)!}{a!0!}$.

Para o passo indutivo basta observar que

$$f_n(a_1,\ldots,a_n)=\sum_{k=1}^{n}f_n(a_1,\ldots,a_k-1,\ldots,a_n)=\sum_{k=1}^{n}\frac{(a_1+\ldots+a_n-1)!}{a_1!\ldots(a_k-1)!\ldots a_n!}=$$
$$\frac{(a_1+\ldots+a_n-1)!}{(a_1-1)!\ldots(a_n-1)!}\sum_{k=1}^{n}\frac{a_k}{a_1\ldots a_n}=\frac{(a_1+\ldots+a_n-1)!}{(a_1-1)!\ldots(a_n-1)!}\frac{a_1+\ldots+a_n}{a_1\ldots a_n}=\frac{(a_1+\ldots+a_n)!}{a_1!\ldots a_n!}.$$

□

Demonstração do Teorema 2.1. Sejam $a_1,\ldots a_m,b_1,\ldots,b_m$ satisfazendo o enunciado. Isso significa que dados os $a_1,\ldots,a_m\in\mathbb{F}_p$ os $a_i's$ precisam ser todos não nulos e os $b_i=a_i+d_i$ também. Além disso, todos os a_i's e b_i's são distintos e logo $a_i-a_j\neq 0$, $b_i-a_j=a_i-a_j+d_i\neq 0$ e $b_i-b_j=a_i-a_j+d_i-d_j\neq 0$, para todo $1\leq i\neq j\leq m$.

Considere o polinômio $f\in\mathbb{F}_p[x_1,\ldots,x_m]$ dado por

$$f(x_1,\ldots,x_m)=x_1\ldots x_m(x_1+d_1)\ldots(x_m+d_m)\prod_{1\leq i<j\leq m}(x_i-x_j)(x_i-x_j+d_i)(x_i-x_j-d_j)(x_i-x_j+d_i-d_j).$$

É fácil ver que f tem grau $m+m+4\binom{m}{2}=2m+2m(m-1)=2m^2=m(p-1)$. Além disso, pelo parágrafo

acima temos que $f(a_1,\dots,a_m) \neq 0$ se, e somente se, $a_1,\dots,a_m$ é uma solução para o nosso problema. Então encontrar uma solução é equivalente a achar um $a \in \mathbb{F}_p^m$ com $f(a) \neq 0$.

Pelo Teorema 1.18 isso é possível se o coeficiente de $x_1^{p-1}\dots x_m^{p-1}$ for diferente de 0. Não é muito difícil ver que o que queremos é o coeficiente de $x_1^{2m-2}\dots x_m^{2m-2}$ em $\prod_{1\leq i<j\leq m}(x_i-x_j)^4$. Isso é o mesmo que achar o coeficiente do termo livre de

$$\frac{1}{x_1^{2(m-1)}\dots x_m^{2(m-1)}}\prod_{1\leq i<j\leq m}(x_i-x_j)^4 = \prod_{1\leq ineqj\leq m}\frac{(x_j-x_i)^2}{x_i^2} = \prod_{1\leq ineqj\leq m}(1-\frac{x_i}{x_j})^2.$$

Usando a conjectura de Dyson para $a_i = 2$ obtemos que esse coeficiente é $\frac{(2m)!}{2^m}$. Como $2m < p-1$ segue que $\frac{(2m)!}{2^m} \neq 0$ em $\mathbb{F}_p$ e portanto existe um $a \in \mathbb{F}_p^m$ com $f(a) \neq 0$. □

Isso resolve o problema de particionar corpos finitos de ordem prima. Para outros corpos finitos ainda não se sabe se é possível. Por exemplo, para corpos de ordem potência de 2 temos a seguinte conjectura.

Conjectura 2.3. *Seja $m = 2^{n-1}$. Dados m elementos $d_1,\dots,d_m \in \mathbb{F}_{2^n}$ se $d_1+\dots+d_m = 0$, então existem $a_1,\dots,a_m,b_1,\dots,b_m \in \mathbb{F}_{2^n}$ distintos tais que*

$$b_i - a_i = d_i \quad \forall\, 1 \leq i \leq m.$$

A próxima aplicação lida com o problema de lista coloração de grafos. Seja G um grafo e C um conjunto de cores. Seja $\mathcal{L} = \{L_v \subset C : v \in V(G)\}$ um conjunto de listas de cores, cada lista associada com um vértice. Dizemos que G é $\mathcal{L}$-colorível se existe $c : V(G) \to C$ tal que $c(x) \neq c(y)$ para todo $\{x,y\} \in E(G)$ e $c(x) \in L_x$ para todo $x \in V(G)$. Isto é, se existe uma coloração própria em que cada vértice usa uma das cores da sua lista.

O número cromático $\chi(G)$ de um grafo G é o menor inteiro k tal que existe uma coloração própria $c : V(G) \to [k]$. O número lista cromático $\chi_L(G)$ é o menor inteiro k tal que para qualquer conjunto $\mathcal{L} = \{L_v : v \in V(G), |L_v| = k\}$ o grafo G é $\mathcal{L}$-colorível. Isto é, k é o menor número tal que para qualquer conjunto de listas de tamanho k existe uma coloração própria em que cada vértice usa uma das cores da lista.

É fácil ver que $\chi_L(G) \geq \chi(G)$, pois podemos escolher todas as listas iguais. Assim uma coloração de G nesse caso nos forneceria uma coloração de G para o problema sem listas. O surpreendente é que esses números não se relacionam tão bem. Considere o seguinte exemplo.

H é um grafo bipartido completo em que cada bipartição é igual a $\binom{[2k-1]}{k}$, ou seja, cada bipartição consiste de todos os k-subconjuntos de $[2k-1]$. É possível ver que $\chi(H) = 2$, porém $\chi_L(H) > k$. De fato, considere $C = [2k-1]$ e para cada vértice $v \in \binom{[2k-1]}{k}$ a lista de cores $L_v = v$. Toda coloração respeitando a lista conterá k cores em cada bipartição, e como o grafo é bipartido completo, pelo princípio da casa dos pombos existe dois vértices de mesma cor adjacente. Então existem grafos G com $\chi(G) = 2$ e $\chi_L(G)$ arbitrariamente grande.

Estamos interessados em estimar $\chi_L(G)$. O problema clássico de estimar $\chi(G)$ é muito conhecido. Uma estimativa inocente nos dá que $\chi(G) \leq \Delta(G)+1$, onde $\Delta(G)$ é o grau máximo de G. Uma forma de se ver isso é procedendo de forma gulosa. Suponha que comecemos a pintar os vértices de G com as cores em $[\Delta(G)+1]$ e agora estamos em um vértice v intermediário. Como $d(v) \leq \Delta(G)$, temos que sempre existe uma cor possível para v diferente da cor de todos os seus vizinhos. Colorímos v com essa cor e prosseguimos. Fazemos isso até pintar todos os vértices e pronto. Essa cota é em algum sentido forte, pois se tomarmos $G = K_r$ temos que $\chi(G) = \Delta(G)+1 = r$ e o mesmo se tomarmos $G = C_{2k+1}$, pois $\chi(G) = \Delta(G)+1 = 3$.

O Teorema de Brooks nos garante que na verdade esses são os dois únicos casos em que ocorrem igualdade.

Teorema 2.4 (Brooks)**.** *Seja G um grafo. Se G não é um grafo completo ou um cíclo ímpar, então $\chi(G) \leq \Delta(G)$.*

A nossa próxima aplicação é o Teorema de Brooks para lista coloração.

Teorema 2.5 (Brooks para lista coloração)**.** *Seja G um grafo. Se G não é um grafo completo ou um cíclo ímpar, então $\chi_L(G) \leq \Delta(G)$.*

Teorema 2.5 é um pouco mais forte que Teorema 2.4. Em particular, porcausa que $\chi_L(G) \geq \chi(G)$ temos que ele implica o teorema de Brooks original.

Podemos modelar o problema para polinômios. Seja G um grafo fixo de n vértices e m arestas. Dado um conjunto $C \subset \mathbb{R}$ de cores, uma coloração pode ser vista como um elemento de C^n. Queremos um polinômio f que devolve 0 se, e somente se, a coloração não é própria. Em geral uma aplicação do Teorema 1.18 nos dará um $x \in C^n$ tal que $f(x) \neq 0$, isso é muito bom pois pela definição de f uma não raiz é uma coloração própria do grafo G. Assim achar um polinômio dessa forma é um bom começo. Um polinômio adequado parece ser $f \in \mathbb{R}[x_1, \ldots, x_n]$ dado por

$$f(x_1, \ldots, x_n) = \prod_{\substack{\{i,j\} \in E \\ i<j}} (x_i - x_j).$$

De fato, uma coloração é própria se, e somente se, todos os fatores desse produtos são diferentes de 0, ou seja, se o polinômio não é nulo. Cada fator contribui em um para o grau, logo $deg(f) = m$. Vamos estudar agora como se comportam os monômios desse polinômio.

Cada monômio de f depende de qual variável nós escolhemos para cada fator $(x_i - x_j)$ no produtório. Cada uma dessas escolhas corresponde a uma orientação do grafo G. Ao escolhermos x_j no termo $(x_i - x_j)$ estamos nos referindo às orientações de G com arco (i, j), isto é, o arco sai de i para j. Ao escolhermos x_i estamos nos referindo às orientações de G com arco (j, i). Seja D uma orientação de G, suponha que $d_D^+(i)$ é o grau de saida do vértice i e que S_D é o número de arcos (i, j) de D tais que $i > j$. Disso podemos ver que a orientação D contribui com o monômio

$$(-1)^{S_D} x_1^{d_D^+(1)} \ldots x_n^{d_D^+(n)}.$$

Dados inteiros $d_1, \ldots, d_n \geq 0$ defina $DE(d_1, \ldots, d_n)$ como o conjunto das orientações D de G com $d_D^+(i) = d_i$ e S_D par e defina $DO(d_1, \ldots, d_n)$ como o conjunto das orientações de G com $d_D^+(i) = d_i$ e S_D ímpar. Temos então que

$$f(x_1, \ldots, x_n) = \sum_{d_1, \ldots, d_n \geq 0} (|DE(d_1, \ldots, d_n)| - |DO(d_1, \ldots, d_n)|) x_1^{d_1} \ldots x_n^{d_n}.$$

Agora fixe uma orientação $D \in DE(d_1, \ldots, d_n) \cup DO(d_1, \ldots, d_n)$. Dado uma orientação qualquer $D' \in DE(d_1, \ldots, d_n) \cup DO(d_1, \ldots, d_n)$ podemos definir $D \oplus D'$ como o subgrafo orientado de D formado pelos arcos que tem orientação diferentes dos de D'. Note que como D e D' concordam em orientação exceto em $D \oplus D'$ e D, D' ambos possuem mesmos graus de entrada e saida, temos então que $D \oplus D'$ é tal que $d^+(x) = d^-(x)$ para todo $x \in V$. Isso significa que $D \oplus D'$ é euleriano, ou seja, suas arestas podems ser particionadas em ciclos. Seja $EE(D)$ o número de subgrafos eulerianos pares de D (com número par de aresta) e $EO(D)$ o número de subgrafos eulerianos ímpares de D. A aplicação $D' \mapsto D \oplus D'$ é uma bijeçao entre $DE(d_1, \ldots, d_n) \cup DO(d_1, \ldots, d_n)$ e os subgrafos eulerianos de D. De fato, dado um subgrafo orientado euleriano F nós podemos construir D' tal que $F = D \oplus D'$. Basta considerar D' como o grafo orientado obtido de D trocando a orientação de todos os arcos em F. A injeção segue simplesmente do fato que duas orientações distintas D', D'' discordam de D em arcos diferentes.

Suponha agora que $D \in DE(d_1, \ldots, d_n)$. Seja $D' \in DE(d_1, \ldots, d_n)$ e seja A_D o número de arcos (i, j) com $i > j$ e (i, j) é um arco de $D \oplus D'$. Defina $B_D = S_D - A_D$. Da mesma forma podemos definir $A_{D'}$ como o número arcos (i, j) de D' com $i > j$ e (j, i) arco de $D \oplus D'$ (lembre que em $D \oplus D'$ os arcos de D e D' estão em direções opostas), também fazemos $B_{D'} = S_{D'} - A_{D'}$. Por coincidirem fora de $D \oplus D'$ é facil ver que $B_D = B_{D'}$. Disso segue que $A_D - A_{D'} = S_D - S_{D'}$. De $S_D, S_{D'}$ possuirem a mesma paridade, segue que $A_D, A_{D'}$ também possuem a mesma paridade. Porém todo aresta $\{i, j\}$ de $D \oplus D'$ é considerada ou em D como um arco (i, j) com $i > j$, ou em D' como um arco (j, i) com $j > i$. Logo $A_D + A_{D'} = E(D \oplus D')$ e dai segue que $D \oplus D' \in EE(D)$. Analogamente podemos ver que se $D' \in DO(d_1, \ldots, d_n)$, então $D \oplus D' \in EO(D)$.

Se supormos que $D \in DO(d_1, \ldots, d_n)$, a análise do parágrafo anterior nos mostra que $D \oplus D' \in EE(D)$ se $D' \in DO(d_1, \ldots, d_n)$ e $D \oplus D' \in EO(D)$ se $D' \in DE(d_1, \ldots, d_n)$. Isso significa que dependendo da paridade de D a nossa aplicação ou manda orientações em subgrafos eulerianos de mesma paridade, ou manda em subgrafos de paridade distinta. Usando da bijeção anterior temos que

$$\big||DE(d_1,\dots,d_n)| - |DO(d_1,\dots,d_n)|\big| = |EE(D) - EO(D)|.$$

Como isso nos é util? Suponha que encontramos uma orientação D de G tal que $EE(D) \neq EO(D)$ e com $d_D^+(i) = d_i$ para todo $1 \leq i \leq n$. Então o coeficiente de $x_1^{d_1} \dots x_n^{d_n}$ em modulo é igual a $|EE(D) - EO(D)| \neq 0$, ou seja, é não nulo. Isso significa que se $L_1, \dots, L_n$ forem listas de cores com $|L_i| = d_i + 1$, entao pelo Nullstellensatz Combinatório (Teorema 1.18) existe $c \in L_1 \times \dots \times L_n$ com $f(c) \neq 0$. Logo c é uma coloração própria de G respeitando as listas. Esses últimos parágrafos provam o que é conhecido como Teorema de Alon-Tarsi

Teorema 2.6 (Alon-Tarsi)**.** *Seja D uma orientação de um grafo G e sejam $\{L_v\}_{v \in V(G)}$ listas tais que $|L_v| \geq d^+(v) + 1$. Se $EE(D) \neq EO(D)$, então existe uma coloração própria de G respeitando as listas.*

Uma observação simples é que por simetria podemos trocar a condição $|L_v| \geq d^+(v) + 1$ por $|L_v| \geq d^-(v) + 1$. Um corolário imediato desse teorema é o seguinte.

Corolário 2.7. *Se G possui uma orientação D tal que $EE(D) \neq EO(D)$ e $d^-(v) \geq 1$ para todo $v \in G$, então $\chi_L(G) \leq \Delta(G)$.*

Demonstração. Basta mostrar que existe uma coloraçao respeitando qualquer lista $\{L_v\}_{v \in V(G)}$, com $|L_v| = \Delta(G)$. Porém como $\Delta(G) = \max\{d^+(v) + d^-(v)\} \geq \max\{d^+(v)\} + 1$ segue que $|L_v| = \Delta(G) \geq d^+(v) + 1$ e logo pelo Teorema de Alon-Tarsi existe uma coloração própria de G respeitando as listas. □

◇ ◇ ◇ *Aula 6 (17 de Outubro) — Lucas Colucci* ◇ ◇ ◇

Provaremos o Teorema 2.5 utilizando o Corolário 2.7. Para isso precisamos encontrar uma orientação apropriada para nosso grafo G. Usaremos de dois lemas na nossa demonstração.

Lema 2.8. *Se G é conexo e $v \in V(G)$ um vértice de G, então existe uma ordenação $v = v_1, \dots, v_n$ dos seus vértices tal que $G[\{v_1, \dots, v_i\}]$ é conexo, para todo $1 \leq i \leq n$.*

Demonstração. Considere uma árvore geradora com raiz em v e ordene os vértices em ordem crescente de distância a v nesta árvore. Essa ordenação funciona pois o subrafo induzido por $v_1, \dots, v_i$ da árvore é conexo, portanto $G[\{v_1, \dots, v_n\}]$ é conexo. □

O próximo lema precisa de algumas definições. Um grafo G é 2-conexo, se para todo $v \in G$ o grafo $G - v$ é conexo, ou seja, G é 2-conexo se é necessario retirar pelo menos dois vértices para ele deixar de ser conexo. Um *bloco* de G é um subgrafo maximal que é 2-conexo. Caso G seja 2-conexo, então o grafo inteiro G é um bloco.

Dado um grafo G qualquer, podemos decompor ele em blocos $B_1, \dots, B_t$. Considere o grafo $B(G)$ obtido por colapsar B_i em um vertice i e tal que $\{i, j\} \in E(B(G))$ se, e somente se, $B_i \cap B_j \neq \varnothing$. Um resultado clássico em teoria dos grafos nos diz que, para todo i, j, os blocos B_i, B_j intersectam em no máximo um vértice e que o grafo $B(G)$ é uma árvore. Podemos assim chamar $B(G)$ de a árvore de blocos de G. O grafo G é uma *árvore de Gallai* se G é conexo e em sua decomposição por blocos $B_1, \dots, B_t$ temos que B_i é ou um ciclo ímpar, ou um grafo completo, para todo $1 \leq i \leq t$. O próximo lema nos dá uma caracterização de árvores de Gallai.

Lema 2.9. *Dado G grafo conexo temos que G é uma árvore de Gallai se, e somente se, G não possui um ciclo par induzido com no máximo uma corda.*

Demonstração. Se G é uma árvore de Gallai, então G não possui um ciclo par induzdo com no máximo uma corda. Todo ciclo par é na verdade um grafo completo. Vamos mostrar agora que todo grafo G que não é uma árvore de Gallai possui um ciclo par induzido com no máximo uma corda. Como G não é uma árvore de Gallai, existe um bloco B de G em que B não é um ciclo ímpar, nem um grafo completo. Vamos achar tal grafo dentro de B.

Seja S um conjunto minimal de vértices tal que $B - S$ é desconexo. Sejam $F_1, \dots, F_t$ as componentes conexas de $B - S$. Pela minimalidade de S temos que $N(x) \cap F_i \neq \varnothing$ para todo $x \in S$. De fato, suponha que exista F_i tal que $N(x) \cap F_i = \varnothing$. Então o grafo $B - \{S \setminus \{x\}\}$ é desconexo, pois caso não fosse, existiria caminho de F_i até x, o que é impossível. Porém isso contradiz a minimalidade de S. Como B é 2-conexo,

temos que $|S| \geq 2$ e existem pelo menos dois vértices $u, v \in S$. Sejam P_1, P_2 dois caminhos mínimos entre u e v, P_1 usando somente vértices em F_1 e P_2 usando somente vértices em F_2. O ciclo $C = P_1 \cup P_2$ é o nosso candidato natural.

A primeira observação é que pela minimalidade de P_1 e P_2 e pelo fato de não existirem arestas entre F_1 e F_2, temos que a única possível corda em C é uv. É fácil também ver que por P_1, P_2 serem caminhos de tamanho pelo menos 2, temos que C é um ciclo de tamanho pelo menos 4. Se C for um ciclo par, então estamos resolvidos. Resta o caso em que C é ciclo ímpar. Neste caso se uv é uma aresta, então $P_1 \cup \{uv\}$ ou $P_2 \cup \{uv\}$ forma um ciclp par induzido. Assim resta considerar C ciclo impar induzido.

Como B não é um cíclo ímpar, segue que $B - C$ é não vazio. Suponha que exista um vértice $x \in B - C$ tal que x possui pelo menos $k \geq 2$ vizinhos em C. Esses k vértices dividem C em k caminhos $C_1, \ldots, C_k$. Suponha que exista um C_i caminho de tamanho par, então $C_i \cup \{x\}$ é um ciclo induzido de tamanho par a não ser que $k = 2$, C_1 é par e C_2 é uma aresta. Neste caso temos que $C_1 \cup \{x\}$ é um ciclo par com uma corda. Portanto podemos assumir que todos os C_i's são caminhos ímpares. Como C é ímpar, isso implica que k também é ímpar. Mas agora note que $C_1 \cup C_2 \cup \{x\}$ é um ciclo par com uma corda, exceto o caso em que $k = 3$ e C_3 é uma aresta. Neste caso, considere os ciclos $C_1 \cup C_3 \cup \{x\}$ e $C_2 \cup C_3 \cup \{x\}$. Para ambos não formarem um ciclo par com uma corda devemos ter também que C_1 e C_2 sejam arestas. Portanto C é um ciclo de tamanho 3, o que é um absurdo.

Então nos resta trabalhar com o caso em que todos os vértices de $B - C$ tem apenas um vizinho em C. Seja P o menor caminho entre dois vértices de C utilizando apenas vértices em $B - C$ e sejam $x, y \in C$ os dois extremos desse caminho. Os dois vértices dividem C em dois caminhos Q_1, Q_2. Como C é ciclo impar segue que $P \cup Q_1$ ou $P \cup Q_2$ é um ciclo par. Suponha que $P \cup Q_1$ seja par. Basta mostrar que este ciclo é induzido. Se existe uma corda em $P \cup Q_1$, pela minimalidade de P essa corda deveria ser entre um vértice $z \in P$ e um vértice $w \in Q_1$. Sejam P', P'' os dois caminhos em que z divide P. Como todo vértice em $B - C$ possui apenas um vizinho em C segue que z não é adjacente nem a x, nem a y. Logo P' e P'' possuem tamanho pelo menos 2. Isso significa que $P' \cup w$ é um caminho menor que P, contradizendo a minimalidade de P. Assim existe um ciclo par com no máximo uma corda em B e como os blocos intersectam em no máximo um vértice, temos um ciclo par com no máximo uma corda em G. □

Podemos agora provar o Teorema de Brooks para lista coloração.

Demonstração do Teorema 2.5. Podemos supor que G é conexo. Além disso podemos supor que G é regular. Suponha que não, então existe um vértice v com $d(v) < \Delta(G)$. Vamos provar então que existe uma coloração própria pra qualquer conjunto de listas $\{L_x\}_{x \in G}$ com $|L_x| = \Delta(G)$ para todo $x \in G$. Considere a ordenação dos vértices $v = v_1, \ldots, v_n$ dada pelo Lema 2.8. Esse lema nos diz que o subgrafo $G[\{v_1, \ldots, v_i\}]$ é conexo, para todo $1 \leq i \leq n$. Em particular, dado v_i podemos afirmar que $N(v_i) \cap \{v_1, \ldots, v_{i-1}\} \neq \emptyset$ para todo $i \geq 2$, ou seja, todo vértice v_i possui um vizinho v_j com $j < i$.

Colorimos gulosamente começando de v_n e indo até $v = v_1$. Suponha que dado algum momento já colorimos $v_n, \ldots, v_{i+1}$ com $i \geq 2$ e queremos colorir agora v_i. Como v_i possui pelo menos um vizinho em $\{v_1, \ldots, v_{i-1}\}$, então o número de vizinhos já pintados é no máximo $d(v_i) - 1 \leq \Delta(G) - 1$. Usando que $|L_{v_i}| = |\Delta(G)|$, existe uma cor disponível para colorimos v_i. Quando $i = 1$ temos que v_1 possui $d(v_1) = d(v) \leq \Delta(G) - 1$ vizinhos coloridos e o mesmo processo é possível. Assim concluimos que $\chi_L(G) \leq \Delta(G)$.

De agora pra frente G é regular. Suponha que G é uma árvore de Gallai. Considere $B_1, \ldots, B_t$ a decomposição de G por blocos, e suponha que B_1 corresponde a uma folha em $B(G)$. Seja B_2 o vizinho de B_1, ou seja, o bloco tal que $|B_1 \cap B_2| = 1$. Então existe um vértice em B_1 que tem grau maior do que os outros. Isso mostra que G só pode ser composto de um bloco, e logo G é um grafo completo ou um ciclo ímpar, o que contradiz a hipótese. Então podemos supor que G não é uma árvore de Gallai e pelo Lema 2.9 possui um ciclo par C com apenas uma corda.

Contraia esse ciclo em um super vértice v e considere a ordenação $v = v_1, \ldots, v_{n-|C|+1}$ dada pelo Lema 2.8. Descontraia o vértice v no ciclo $x_1, \ldots, x_{|C|}$. Vamos agora orientar G da seguinte forma, para uma aresta $\{v_i, v_j\}$ com $1 < i < j \leq n - |C| + 1$ considere o arco (v_i, v_j). Para arestas da forma $\{x_i, v_j\}$ considere o arco (x_i, v_j). Por fim oriente as arestas de C respeitando o ciclo, isto é, $(x_1, x_2), \ldots, (x_{|C|}, x_1)$ e a corda em qualquer orientação. É possível ver que essa orientação D obtida satisfaz a condição de que $d^-(x) \geq 1$ para todo $x \in G$. De fato, isso é verdade para todo vértice em C e pelo Lema 2.8, todo vértice v_i possui um vizinho ou em C ou v_j com $j < i$ e daí $d^-(v_i) \geq 1$.

Assim para aplicarmos o Corolário 2.7. só precisamos mostrar que $EE(D) \neq EO(D)$. Um digrafo euleriano é uma união de ciclos, como os únicos ciclos em D estão em C só precisamos só temos no máximo 3 possíveis digrafos. Se C é um ciclo par induzido, os únicos subrafos eulerianos seriam C e o conjunto vazio. Daí $EE(D) = 2 \neq 0 = EO(D)$. Caso C possua uma corda, sua corda divive em dois ciclos menores C_1 e C_2. Apenas um deles é euleriano, o que depende da orientação da corda. Juntos com C e o conjunto vazio, esses são os únicos subgrafos eulerianos de D. Mas aí no pior caso teriamos $EE(D) = 2 \neq 1 = EO(D)$. Logo podemos aplicar o Corolário 2.7 e segue que $\chi_L(G) \leq \Delta(G)$. □

Vamos ver agora outras aplicações do Teorema de Alon-Tarsi. Relembrando, o teorema basicamente nos diz que se acharmos uma orientação D de G com $EE(D) \neq EO(D)$, então $\chi_L(G) \leq \max_{v \in G}\{d_D^+(v)\} + 1$. Então estamos interessados em dois problemas, o de achar uma orientação com grau de saida máximo pequeno e o de achar uma orientação com número de subgrafos eulerianos ímpares e pares distintos. O que acontece se considerarmos uma família em que o segundo problema é sempre verdade? Então poderiamos nos dedicar a resolver o problema de minimizar o grau de saida sem restrições. Isso é o que acontece quando tomamos G como um grafo bipartido. Por um grafo bipartido não conter ciclos ímpares e todo grafo euleriano ser uma união de ciclos, temos que para qualquer orientação D de G vale $EO(D) = 0 \neq 1 \leq EE(D)$ (Lembre se que o conjunto vazio é um subgrafo euleriano par). Assim uma aplicação imediata do Teorema 2.7 nos dá que

Teorema 2.10. *Seja G um grafo bipartido e D uma orientação de G, então vale que $\chi_L(G) \leq \max_{v \in G}\{d_D^+(v)\} + 1$.*

Precisamos agora encontrar uma orientação que minimize o grau de saída máximo. Para fazermos isso vamos precisar usar um resultado clássico em teoria dos grafos, o Teorema de Hall. Dado um grafo bipartido $G = (A, B)$ com $|A| \geq |B|$ dizemos que G satisfaz a *condição de Hall* se para todo $X \subset A$, temos que $|N(X)| \geq X$. Um emparelhamento de um grafo G é um conjunto de arestas M tal que nenhuma aresta compartilha vértices. Quando G é bipartido dizemos que um emparelhamento é *perfeito* se todo vértice da menor bipartição (no caso A) está em uma aresta do emparelhamento. O Teorema de Hall nos diz que a condição de Hall é necessária e suficiente para garantir um emparelhamento máximo.

Teorema 2.11 (Hall)**.** *Seja $G = (A, B)$ um grafo bipartido. Então G possui um emparelhamento perfeito, se e somente se, G satisfaz a condiçao de Hall.*

Vamos definir agora uma noção de densidade de grafos. Dado um grafo G definimos

$$L(G) = \max_{H \subset G} \frac{e(H)}{v(H)}$$

como a maior densidade de um subgrafo de G. O próximo lema responde o nosso problema em função desse parâmetro $L(G)$.

Lema 2.12. *G admite orientação D no qual $d_D^+(v) \leq d$, para todo $v \in G$, se, e somente se, $L(G) \leq d$.*

Demonstração. Suponha que D é uma orientação com $d_D^+(v) \leq d$, para todo $v \in G$. Então para todo $H \subset G$ temos que

$$e(H) = \sum_{v \in H} d_{D(H)}^+(v) \leq \sum_{vinH} d_D^+(v) \leq dv(H).$$

Do que segue

$$\frac{e(H)}{v(H)} \leq d$$

para todo $H \subset G$ e logo $L(G) \leq d$.

Agora suponha que $L(G) \leq d$. Construa o seguinte grafo bipartido $F = (A, B)$. O conjunto $A = E(G)$, ou seja, os vértices da partição A são as arestas de G. O conjunto $B = V_1 \cup \ldots \cup V_d$ onde $V_1, \ldots, V_d$ são d cópias de $V(G)$. Dado $e \in A, u \in B$, temos que $\{e, u\}$ é uma aresta se u é uma cópia de um vértice pertencente a aresta e. É fácil ver que toda aresta $e \in A$ contém exatamente $2d$ vizinhos em B. Além disso, como $L(G) \leq d$, temos que $|A| = e(G) \leq dv(G) = |B|$. Vamos mostrar que F satisfaz a condição de

Hall. Seja $X \subset A$ um subconjunto de arestas de G. O conjunto X corresponde a um subgrafo $H \subset G$. Disso não é difícil ver que a vizinhança de X consiste das cópias dos vértices de H. Usando da definição de $L(G)$ obtemos que

$$|N(X)| = dv(H) \geq e(H) = |X|.$$

Portanto pelo Teorema de Hall temos que F possui um emparelhamento perfeito. Isto é, cada aresta de $E(G)$ está emparelhada com uma cópia de um vértice dessa aresta. Se uma aresta uv está conectada com uma cópia de v escolha o arco (v,u). Caso contrário, escolha o arco (u,v). Assim obtemos uma orientação D de G de acordo com esse emparelhamento. Resta mostrar que essa orientação satisfaz o desejado.

Para isso basta notar que o grau de saida de um vértice v nessa orientação é exatamente o número de cópias desse vértice que estão contidas em alguma aresta do emparelhamento. Como no total temos no máximo d cópias, segue que $d_D^+(v) \leq d$. □

Aplicando esse resultado ao Teorema 2.10 obtemos que

Teorema 2.13. *Se G é um grafo bipartido, então $\chi_L(G) \leq \lceil L(G) \rceil + 1$.*

Esse resultado é o melhor possível no sentido em que existe grafo bipartido em que ocorre a igualdade. De fato considere o grafo $G = K_{t,t^t}$, isto é, o grafo bipartido completo cuja as bipartições $G = (A,B)$ tem tamanho $A = [t]$ e $|B| = [t]^t$. Para calcular $L(G)$ temos

$$L(G) = \max_{\substack{A' \subset A \\ B' \subset B}} \frac{e(A',B')}{|A'|+|B'|} = \max_{\substack{0 \leq a \leq t \\ 0 \leq b \leq t^t}} \frac{ab}{a+b} = \max_{\substack{0 \leq a \leq t \\ 0 \leq b \leq t^t}} \frac{1}{\frac{1}{a}+\frac{1}{b}} = \frac{1}{\frac{1}{t}+\frac{1}{t^t}} \leq t$$

Portanto pelo último teorema $\chi_L(G) \leq t+1$. Vamos provar agora que $\chi_L(G) = t+1$. Para isso considere as listas $L_i = \{t(i-1)+1, \ldots, t(i-1)+t\}$ para todo $1 \leq i \leq t$ e as listas $L_{(i_1,\ldots,i_t)} = \{i_1, t+i_2, 2t+i_3, \ldots, t(t-1)+i_t\}$ para todo $(i_1,\ldots,i_t) \in [t]^t$. Suponha que exista uma coloração própria c respeitando a lista e $c(1) = b_1$, $c(2) = t+b_2, \ldots, c(t) = t(t-1)+b_t$ são as cores dos elementos de A. Então essas cores correspondem a lista de $(b_1,\ldots,b_t) \in B$, o que significa que não existe cor disponível para esse vértice, absurdo! Assim G é um exemplo de grafo bipartido em que ocorre a igualdade.

Por fim, para algumas famílias de grafos bipartido podemos garantir que $L(G)$ é pequeno e logo obter boas cotas para o número lista cromático. Esse é o caso dos grafos bipartidos planares.

Lema 2.14. *Se G é grafo bipartido planar, então $e(G) \leq 2v(G) - 4$.*

Demonstração. Considere uma representação planar de G. Essa representação possui $a = e(G)$ arestas, f faces e $v = v(G)$ vértices. A fórmula de Euler nos garante que

$$v - a + f = 2.$$

Como o grafo é bipartido sabemos que não existem faces triangulares nessa representação. Vamos agora contar o número S de pares (e,F) onde e é uma aresta na face F. Podemos contar isso de duas formas. Se fixarmos uma aresta, existem exatamente duas faces compartilhando essa aresta e logo $S = 2a$. Se fixarmos uma face existem no mínimo 4 arestas contidas nesta face e logo $S \geq 4f$. Juntando os dois resultados obtemos $f \leq a/2$. Substituindo na forma de Euler obtemos o resultado desejado. □

Teorema 2.15. *Se G é grafo bipartido planar, entao $\chi_L(G) \leq 3$.*

Demonstração. Pelo lema anterior, e usando que subgrafo de grafo bipartido planar é também bipartido planar, temos que

$$L(G) = \max_{H \subset G} \frac{e(H)}{v(H)} = \max_{H \subset G} \frac{2v(H)-4}{v(H)} \leq 2.$$

O resultado agora sai usando o Teorema 2.13. □

3 Polinômios Cromáticos de Grafos

◇ ◇ ◇ *Aula 7 (24 de Outubro) — Yoshiharu Kohayakawa* ◇ ◇ ◇

Vamos estudar nessa seção o polinômio cromático de um grafo. Seja G um grafo simples de n vértice, isto é, um grafo em que no máximo uma aresta sai de cada par de vértices e não existem loops. Uma coloração $c : V(G) \to C$ de G é própria se para toda aresta $\{x, y\} \in E(G)$ temos que $c(x) \neq c(y)$. O número cromático de G pode ser definido como

$$\chi(G) = \min\{k \in \mathbb{N} : \text{ existe coloração própria } c : V(G) \to [k]\}$$

o menor inteiro k para qual existe uma coloração própria de G com k cores.

O problema de determinar o número cromático de G foi bastante estudado na literatura. Aqui vamos nos focar em um problema relacionado, o problema de determinar o número de colorações próprias de G com λ cores. Defina $\gamma(G, \lambda)$ como o número de colorações $c : V(G) \to [\lambda]$ próprias distintas de G, onde λ é um inteiro. A primeira coisa a notar é que essa função é um polinômio em λ.

Proposição 3.1. *Para todo grafo G a função $\gamma(G, \lambda)$ é um polinômio em λ.*

Demonstração. Dizemos que uma partição $P = \{P_i\}_{i \in I}$ de G é uma partição em conjuntos independentes se

1. $V(G) = \bigcup_{i \in I} P_i$
2. $P_i \cap P_{i'} = \varnothing$, para $i, i' \in I$.
3. P_i é um conjunto independente em G para todo $i \in I$.

É fácil ver que toda coloração própria de G determina uma partição independente de G, isto é, o conjuntos dos vértices de mesma cor forma uma partição independente. Assim basta calcular o número de colorações para uma partição não ordenada de G. Seja $P = \{P_i\}_{i \in I}$ uma dessas partições e suponha que queremos colorir cada P_i com uma cor distinta entre as cores de $[\lambda]$. Uma contagem simples nos mostra que existem

$$(\lambda)_{|P|} = \lambda(\lambda - 1) \dots (\lambda - |P| + 1)$$

maneiras de colorir as partes dessa partição se $\lambda \geq |P|$. Caso $\lambda < |P|$ a fórmula acima também funciona, pois a expressão terá valor 0 que é exatamente o número de maneiras de colorir a partição.

Então temos que

$$\gamma(G, \lambda) = \sum_{\substack{P \text{ part.} \\ \text{indep. de } G}} \lambda(\lambda - 1) \dots (\lambda - |P| + 1).$$

Como G é finito, o número de partições também é. Isso significa que o lado direito pode ser escrito como um polinômio $p \in \mathbb{R}[x]$ com $\gamma(G, \lambda) = p(\lambda)$, o que conclui a demonstração. □

Denotamos o polinômio da proposição como o polinômio cromático $P_G(\lambda)$ de G. Em geral esse polinômio é díficil de calcular. Uma das razões para isso é que sabemos que se $P_G(k) > 0$ para algum inteiro positivo k, então G pode ser colorido com k cores e logo $\chi(G) \leq k$. Assim calcular o polinômio cromático nos permitiria em essência calcular o número cromático de G que sabemos que é um problema difícil. Apesar disso a próxima proposição mostra uma fórmula mais palatável para $P_G(\lambda)$. Dado um subconjunto T de $E(G)$ nós definimos $c(T)$ como o número de componentes conexas do subgrafo $G_T = (V(G), T)$ cujo os vértices são $V(G)$ e as arestas T.

Proposição 3.2. *Dado G um grafo, temos que*

$$P_G(\lambda) = \sum_{T \subseteq E(G)} (-1)^{|T|} \lambda^{c(T)}.$$

Para provarmos essa proposição vamos precisar do princípio da inclusão e exclusão. O princípio permite calcular a união de uma família de conjuntos dado o tamanho de suas intersecções.

Teorema 3.3 (Inclusão-Exclusão)**.** *Sejam $A_1, \ldots, A_n \subset S$ subconjuntos de um universo S. Então*

$$|S \setminus (\bigcup_{i=1}^{n} A_i)| = \sum_{I \subset [n]} (-1)^{|I|} |A_I|.$$

Onde $A_I = \bigcap_{i \in I} A_i$ e $A_\varnothing = S$.

Demonstração. Para um conjunto $B \subset S$ considere a função $\mathbb{1}_B : S \to \{0,1\}$ dada por

$$\mathbb{1}_B(s) = \begin{cases} 1, & \text{se } s \in B \\ 0, & \text{se } s \notin B \end{cases}, \quad \forall\, s \in S.$$

Nós podemos calcular o tamanho de um conjunto B pelo produto interno $\langle \mathbb{1}_B, \mathbb{1} \rangle$, onde $\mathbb{1}$ é o vetor cujo todas as coordenadas tem valor 1. Agora note que

$$\mathbb{1}_{A_I} = \prod_{i \in I} \mathbb{1}_{A_i}$$

e que

$$\mathbb{1}_{S \setminus \bigcup_{i=1}^{n} A_i} = \prod_{i=1}^{n} (1 - \mathbb{1}_{A_i})$$

Abrindo a útlima expressão temos que

$$\mathbb{1}_{S \setminus \bigcup_{i=1}^{n} A_i} = \sum_{I \subset [n]} (-1)^{|I|} \prod_{i \in I} \mathbb{1}_{A_i} = \sum_{I \subset [n]} (-1)^{|I|} \mathbb{1}_{A_I}$$

tomando o produto interno com $\mathbb{1}$ dos dois lados nós obtemos exatamente a igualdade desejada. □

Demonstração da Proposição 3.2. Precisamos definir quem são os conjuntos para aplicar o Teorema da Inclusão-Exclusão. É natural tomar como S o conjunto de todas as $[\lambda]^{V(G)}$ colorações de G. Vamos indexar os conjuntos pelas arestas de G. Para todo $e \in E(G)$ o conjunto A_e corresponde as colorações de G em que os vértices de e são de mesma cor. De forma a obtermos algo análogo ao enunciado definimos $A_\varnothing = S$, ou seja, todas as colorações possíveis. Seja $T \subset E(G)$ podemos definir $A_T = \bigcap_{e \in T} A_e$ exatamente como preciso. Não é díffícil ver que A_T corresponde ao conjunto de colorações em que todos os vértices em arestas de T possuem mesma cor. Para podermos aplicar o Teorema anterior só resta calcular o tamanho de A_T. Note que em uma componente conexa de T todos os elementos possuem a mesma cor, porque em toda aresta os vértices tem a mesma cor. Assim só precisamos escolher as cores das componentes conexas e logo $|A_T| = \lambda^{c(T)}$. Aplicando o princípio da Inclusão-Exclusao obtemos que

$$|S \setminus (\bigcup_{i=1}^{n} A_i)| = \sum_{T \subseteq E(G)} (-1)^{|T|} \lambda^{c(T)}.$$

Porém $S \setminus (\bigcup_{i=1}^{n} A_i)$ corresponde as colorações em que não existem arestas com vértices da mesma cor, ou seja, as colorações próprias. Logo $P_G(\lambda) = |S \setminus (\bigcup_{i=1}^{n} A_i)|$. □

Porém essa fórmula depende de calcular as componentes conexas de todos os subconjuntos de $E(G)$ o que é impraticavel se G é muito grande. Podemos também obter $P_G(\lambda)$ recursivamente. Para isso precisamos definir uma deleção e uma contração de aresta. Dado um grafo G e uma aresta e de G, o grafo $G - e$ é o grafo obtido ao deletar a aresta e de G, isto é, é o grafo em que o conjunto de arestas é $E(G) \setminus \{e\}$. O grafo G/e é o grafo obtido ao contrair a aresta e. O processo de contração pode ser descrito da seguinte forma. Seja $e = xy$, o grafo G/e contém como conjunto de vértices $(V(G) \cup \{z\}) \setminus \{x, y\}$, ou seja, substituimos os vértices x e y por um novo vértice z. Para o conjunto de arestas retiramos todas as arestas adjacentes a x e a y e para cada aresta da forma $\{x, w\}$ ou $\{y, w\}$ adicionamos a aresta $\{z, w\}$, ou seja, z possui como vizinhança a união $(N_G(x) \setminus \{y\}) \cup (N_G(y) \setminus \{x\})$. A recorrência então é dada como se segue.

Proposição 3.4. *Para todo G e $e \in E(G)$ vale que,*

$$P_G(\lambda) = P_{G-e}(\lambda) - P_{G/e}(\lambda).$$

Demonstração. Suponha que $e = xy$. Considere todas as colorações próprias de $G - e$. Podemos dividir elas em dois tipos. As que x e y possuem cores distintas ou as que x e y possuem mesma cor. É fácil ver que o número de colorações do primeiro tipo é exatamente o número de colorações de G e a do segundo tipo é o número de colorações de G/e. Portanto

$$P_{G-e}(\lambda) = P_G(\lambda) + P_{G/e}(\lambda).$$

□

Note que o resultado acima continua válido se G é um multigrafo e se existem outras arestas além de $e = xy$ conectando x e y. De fato, é fácil ver que G/e possui um loop. Isto significa que não existe coloração própria par G/e e portanto $P_{G/e}(\lambda) = 0$. Agora $G - e$ apesar de ser um multigrafo diferente de G, pode ser visto como o mesmo grafo que G e logo qualquer coloração possível em um, também é possível no outro. Isso implica $P_{G-e}(\lambda) = P_G(\lambda)$ e logo a igualdade da proposição é verdadeira. Vamos agora calcular o polinômio cromático para alguns exemplos.

Exemplo 3.5. Suponha que $G = K_n$, o grafo completo. Nesse caso temos que todas os vértices de G possuem cores distintas. Daí é fácil concluir que $P_G(\lambda) = \lambda(\lambda-1)\dots(\lambda-(n-1))$.

Exemplo 3.6. Suponha que G é uma árvore de n vértices. Para calcularmos o número cromático fixe uma raiz e ordene os vértices em ordem crescente de acordo com sua distância a raiz. É fácil ver que nessa ordenação todo vértice, exceto o primeiro, possui exatamente um vizinho antecedendo ele na ordenação. Pinte os vértices de acordo com essa ordenação. Para o primeiro vértice temos λ possibilidade, para os demais $\lambda - 1$ (porque já existe um vértice vizinho pintado). Logo temos que $P_G(\lambda) = \lambda(\lambda-1)^{n-1}$.

Exemplo 3.7. Suponha que $G = C_n$, o ciclo de $n \leq 3$ vértices. Para calcularmos esse vamos usar a Proposição 3.4. Note que dado uma aresta e de G temos que $G/e = C_{n-1}$ e $G - e = P_n$ o caminho de n vértices. Como P_n é uma árvore, sabemos pelo exemplo anterior o seu polinômio cromático. Assim obtemos que

$$P_{C_n}(\lambda) = \lambda(\lambda-1)^{n-1} - P_{C_{n-1}}(\lambda).$$

Aplicando essa recursão diversas vezes obtemos

$$P_{C_n}(\lambda) = \lambda(\lambda-1)^{n-1} - \lambda(\lambda-1)^{n-2} + \dots + (-1)^{n-3}\lambda(\lambda-1)^2 + (-1)^{n-2}P_{C_2}(\lambda).$$

Podemos interpretar C_2 como um K_2 e logo $P_{C_2}(\lambda) = \lambda(\lambda-1)$. Assim

$$P_{C_n}(\lambda) = \lambda(\lambda-1)^{n-1} - \lambda(\lambda-1)^{n-2} + \dots + (-1)^{n-2}\lambda(\lambda-1) = (\lambda-1)^n + (-1)^n(\lambda-1).$$

Exemplo 3.8. Suponha que G é uma roda de n vértices. O grafo G consiste de um ciclo C_{n-1} e um vertice x conectado a todos os vértices de C_{n-1}. Para calcular o polinômio cromático de G note que x pode ser pintado de λ cores. Assim sobram $(\lambda-1)$ cores pra C_{n-1} e usando do exemplo anterior temos que

$$P_G(\lambda) = \lambda P_{C_{n-1}}(\lambda-1) = \lambda(\lambda-2)^{n-1} + (-1)^{n-1}\lambda(\lambda-2).$$

Exemplo 3.9. Suponha que G seja um grafo e $G_1, \dots, G_t$ sejam suas componentes conexas. Então é possível calcular o polinômio cromático de G em função dos de $G_1, \dots, G_t$. De fato como a coloraçao em todas as componentes conexas são independentes é fácil ver que

$$P_G(\lambda) = P_{G_1}(\lambda)\dots P_{G_t}(\lambda).$$

Exemplo 3.10. Suponha que G é um grafo e seja $B_1, \dots, B_t$ seus blocos em sua decomposição por blocos. Lembre que um bloco é uma componente 2-conexa maximal de G. Blocos de G se intersectam

em no máximo um vértice e se considerarmos o grafo em que os vértices são os blocos e dois blocos são adjacentes se possuem intersecção, então esse grafo é uma árvore. Vamos provar por indução no número de blocos que

$$P_G(\lambda) = \frac{1}{\lambda^{t-1}} P_{B_1}(\lambda) \dots P_{B_t}(\lambda).$$

A afirmação é verdadeira para $t = 1$, ou seja, grafos com apenas um bloco. Suponha sem perda de generalidade que B_t é um bloco correspondente a uma folha na árvore de blocos. Seja G' o grafo obtido pela união dos blocos $B_1, \dots, B_{t-1}$. Qualquer coloração de G' intersecta em B_t em apenas um vértice. Isso significa que precisamos determinar o número de colorações de B_t onde um vértice tem cor fixa.

Existe uma clara bijeção entre colorações em que um vértice x tem cor i ou j. Basta apenas trocar todo vértice de cor i para cor j e vice-versa. Isso nos permite notar que o número de colorações com um vértice de cor fixa é igual para qualquer que seja essa cor. Logo temos que

$$P_G(\lambda) = P_{G'}(\lambda) \frac{P_{B_t}(\lambda)}{\lambda}.$$

Como por indução $P_{G'}(\lambda) = \frac{1}{\lambda^{t-2}} P_{B_1}(\lambda) \dots P_{B_{t-1}}(\lambda)$, o resultado segue.

A próxima proposição nos permite entender melhor o polinômio cromático.

Proposição 3.11. *Seja G um grafo de n vértices. Então*

$$P_G(x) = x^n - a_{n-1}x^{n-1} + \dots + (-1)^{n-1} a_1 x,$$

onde $a_i \geq 0$ para todo $1 \leq i \leq n-1$, $a_{n-1} = e(G)$ e $a_1 = |A - B|$, onde A é o número de subgrafos pares geradores de G e B o de subgrafos ímpares. Além disso, se G é conexo, então vale que $a_i > 0$ para todo $1 \leq i \leq n-1$.

Demonstração. Pela Proposição 3.2 o único termo do somatório $\sum_{T \subset E(G)} (-1)^{|T|} x^{c(T)}$ que contribui para o coeficiente de x^n é quando $T = \varnothing$. Logo P_G é um polinômio mônico. Como o número de componentes conexas é sempre maior do que 0, também segue dessa proposição que o termo independente é 0 e logo 0 é raiz de P_G.

Para calcular a_{n-1} temos que determinar todos os conjuntos T em que $c(T) = n-1$. Esses conjuntos T são exatamente as arestas de $E(G)$, logo $a_T = (-1) \sum_{e \in E(G)} (-1)^1 = e(G)$. Para calcular a_1 temos que determinar todos os conjuntos T em que $c(T) = 1$, ou seja, os subgrafos geradores de G. Uma simples conta nos mostra que

$$|a_1| = |\sum_{T \subset E(G)} (-1)^{|T|}| = |\sum_{T \text{ gerador par}} 1 - \sum_{T \text{ gerador ímpar}} 1| = |A - B|.$$

Resta mostrar que $a_i \geq 0$ para todo $1 \leq i \leq n-1$. Para isso façamos indução no número de arestas e vértices de um grafo. Como caso base tome o grafo G vazio, para este caso temos que $P_G(x) = x^n$, que satisfaz as condições do enunciado. Suponha agora que queremos provar para um grafo G qualquer e o resultado já foi provado para todo grafo H com menos vértices do que G, ou caso H tenha o mesmo número de vértices, para todo H com menos arestas do que G. A Proposição 3.4 nos diz que para uma aresta e em G vale

$$P_G(x) = P_{G-e}(x) - P_{G/e}(x).$$

Por hipótese de indução temos que

$$P_{G_e} = x^n - b_{n-1}x^{n-1} + \dots + (-1)^{n-1} b_1 x,$$
$$P_{G/e} = x^{n-1} - c_{n-2}x^{n-2} + \dots + (-1)^{n-1} c_1 x,$$

onde $b_1, \dots, b_{n-1}, c_1, \dots, c_{n-2} \geq 0$. Disso seque que

$$P_G(x) = (x^n - b_{n-1}x^{n-1} + \dots + (-1)^{n-1} b_1 x) - (x^{n-1} - c_{n-2}x^{n-2} + \dots + (-1)^{n-1} c_1 x) =$$
$$x^n - (b_{n_1} + 1)x^{n-1} + (b_{n-2} + c_{n-2})x^{n-2} + \dots + (-1)^n (b_1 + c_1)x.$$

Logo $a_i = b_i + c_i \geq 0$ para todo $1 \leq i \leq n-2$ e $a_{n-1} = b_{n-1} + 1 > 0$.

Se G é conexo podemos argumentar da mesma maneira para provar que $a_i > 0$ para todo $1 \leq i \leq n-1$. Uma das mudanças é que o caso base da indução tem de ser uma árvore e daí pelo Exemplo 3.6 segue

$$P_G(x) = x(x-1)^{n-1} = \sum_{i=1}^{n} \binom{n-1}{i-1} (-1)^{n-i} x^i.$$

Logo $a_i = (-1)^{n-i}\binom{n-1}{i-1}(-1)^{n-1} = \binom{n-1}{i-1} > 0$. A outra mudança é que para mantermos a hipótese de indução devemos escolher uma aresta e tal que $G-e$ e G/e sejam conexos, mas isso é sempre possível se G é conexo e diferente de uma árvore (basta tomar uma aresta de um ciclo de G). □

Dois corolários imediatos da proposição anterior são os seguintes.

Corolário 3.12. *Dado um grafo G a multiplicidade de 0 em $P_G(x)$ é exatamente o número de componentes conexas de G*

Demonstração. A proposição 3.11 nos mostra que se G é conexo, então 0 tem multiplicidade 1 em $P_G(x)$. Utilizando que o polinômio cromático de um grafo é o produto dos polinômios cromáticos das suas componentes conexas, o resultato segue. □

Corolário 3.13. *Seja G um grafo conexo. Se G possui um número par de vértices, então o número de subgrafos geradores pares é menor do que o número de subgrafos geradores ímpares. Se G possui um número ímpar de vértices, então o número de subgrafos geradores pares é maior do que o número de subgrafos geradores ímpares.*

◇ ◇ ◇ *Aula 8 (31 de Outubro) — Lucas Colucci* ◇ ◇ ◇

Na aula de hoje vamos provar o Teorema da Razão Áurea. O teorema nos permite estimar um pouco o polinômio cromático de um grafo planar em um valor apropriado.

Teorema 3.14 (Tutte)**.** *Seja $\phi = \frac{1+\sqrt{5}}{2}$ a razão áurea e G um grafo planar. Então vale que $P_G(\phi+2) > 0$.*

Como já observado antes, se provarmos que $P_G(k) > 0$ para algum inteiro k, então $\chi(G) \leq k$. Assim podemos tentar determinar o número cromático de um grafo entendendo o seu polinômio cromático. Um dos grandes resultados em teoria dos grafos é o Teorema das quatro cores. Esse teorema afirma que para todo grafo planar G vale que $\chi(G) \leq 4$, ou que $P_G(4) > 0$. O Teorema da razão áurea nos diz que $P_G(\phi+2) > 0$, onde $\phi + 2 \approx 3,618...$. O que é de certa forma um resultado próximo do desejado.

Para provarmos esse teorema vamos precisar de uma série de lemas preliminares relacionados ao estudo do polinômio cromático.

Lema 3.15. *Dado um grafo G, o polinômio P_G não possui raízes em $(0,1)$.*

Demonstração. Podemos supor sem perda de generalidade que G é conexo e possui n vértices. Isso acontece pois o polinômio cromático de G é o produto dos polinômios cromáticos de suas componentes. Assim se nenhum deles possui raízes em $(0,1)$, o polinômio de G também não possuirá. Seja $\alpha \in (0,1)$. Vamos mostrar por indução no número de vértices e arestas de G que $(-1)^{n-1}P_G(\alpha) > 0$. O caso base é quando G é uma árvore. Nesse caso temos pelo Exemplo 3.6 que

$$(-1)^{n-1}P_G(\alpha) = (-1)^{n-1}\alpha(\alpha-1)^{n-1} = \alpha(1-\alpha)^{n-1} > 0.$$

Agora queremos provar o resultado para um grafo G conexo diferente de uma árvore e suponha que já provamos para todo grafo H com menos vértices ou, se H tiver o mesmo número de vértices, com menos arestas do que G. Como G é conexo diferente de uma árvore, G contém um ciclo. Seja e uma aresta desse ciclo. Podemos ver que $G-e$ e G/e são conexos. Aplicando a Proposição 3.4 e a hipótese de indução temos que

$$(-1)^{n-1}P_G(\alpha) = (-1)^{n-1}(P_{G-e}(\alpha) - P_{G/e}(\alpha)) = (-1)^{n-1}P_{G-e}(\alpha) + (-1)^{n-2}P_{G/e}(\alpha) > 0.$$

Isso conclui que $P_G(\alpha) \neq 0$, como queríamos. □

Esse resultado nos permite concluir o seguinte.

Lema 3.16. *O número $\phi + 1 = \frac{3+\sqrt{5}}{2}$ não é raiz de nenhum polinômio cromático.*

Demonstração. Suponha que exista grafo G tal que $P_G(\phi + 1) = 0$. Sabemos pela construção de P_G que $P_G \in \mathbb{Z}[x]$. Considere agora o ideal de polinômios $I = \{f \in \mathbb{Z}[x] : f(\phi + 1) = 0\}$. Vamos mostrar que $I = (b)$ onde $b(x) = x^2 - 3x + 1$. Primeiro observe que $b \in I$, de fato

$$b(\phi + 1) = (\phi + 1)^2 - 3(\phi + 1) + 1 = \phi^2 - \phi - 1 = 0.$$

Agora seja $a \in I$ um elemento qualquer. É fácil ver pelo algoritmo da divisão euclideana e por b ser um polinômio mônico que existem polinômios $q, r \in \mathbb{Z}[X]$ tai que $a = bq + r$ e $deg(r) < deg(b)$. Como $a, b \in I$ seque que $r \in I$. Então $deg(r) \in \{0, 1\}$. Se r for um polinômio de grau 1, então ele é múltiplo de $x - \phi - 1$ e como $\phi + 1$ é irracional segue que $r \notin \mathbb{Z}[x]$, contradição. Logo r possui grau 0 e logo é uma constante. Como $r(\phi + 1) = 0$, seque que r é identicamente nulo. Isso significa que $a = bq$, ou seja, a é um múltiplo de b.

Usando esse resultado podemos afirmar que $P_G(x)$ é um múltiplo de $x^2 - 3x + 1$. Porém $0 < \frac{3-\sqrt{5}}{2} < 1$ é outra raiz de $x^2 - 3x + 1$. Logo $P_G(\frac{3-\sqrt{5}}{2}) = 0$, o que contradiz o Lema 3.15. □

O próximo lema nos fornece relações com o polinômio cromático e certos tipos de grafos planares.

Lema 3.17. *Seja G um grafo planar com uma face quadrilateral F. Sejam e_1, e_2 as diagonais de F e $G_i = G + e_i, i = 1, 2$. Então*

(i) $P_{G_1}(\lambda) + P_{G_1/e_1}(\lambda) = P_{G_2}(\lambda) + P_{G_2/e_2}(\lambda)$

(ii) $P_G(\phi + 1) = (\phi + 1)(P_{G_1}(\phi + 1) + P_{G_2}(\phi + 1))$, *onde* $\phi = \frac{1+\sqrt{5}}{2}$.

Demonstração. (i) Usando a Proposição 3.4 para G_1 com aresta e_1 temos

$$P_{G_1}(\lambda) + P_{G_1/e_1}(\lambda) = P_{G_1 - e_1}(\lambda) = P_G(\lambda).$$

De maneira análoga temos

$$P_{G_2}(\lambda) + P_{G_2/e_2}(\lambda) = P_{G_2 - e_2}(\lambda) = P_G(\lambda).$$

e daí o resultado segue.

(ii) Vamos provar por indução no número de vértices e arestas de G. Primeiro temos que resolver o caso base. Suponha inicialmente que $V(G) = V(F)$, ou seja, os únicos vértices são os vértices da face quadriláteral. Existem duas opçoes para G, ou $G = C_4$, ou G é um C_4 mais uma corda (diamante).

Se $G = C_4$, então tanto G_1 quanto G_2 são diamantes. Uma simples conta nos mostra que

$$P_{G_1}(\lambda) = P_{G_2}(\lambda) = \lambda(\lambda - 1)(\lambda - 2)^2.$$

Além disso, pelo Exemplo 3.7 temos que

$$P_G(\lambda) = (\lambda - 1)^4 + (\lambda - 1).$$

Calculando obtemos então que

$$P_G(\phi + 1) = (\phi + 1)(P_{G_1}(\phi + 1) + P_{G_2}(\phi + 1)) \Leftrightarrow \phi^4 + \phi = 2(\phi + 1)^2\phi(\phi - 1)^2 \Leftrightarrow \phi^3 + 1 = 2(\phi^2 - 1)^2.$$

Agora observe que ϕ é raiz do polinômio $x^2 - x - 1$. Isso significa que $\phi^2 = \phi + 1$. Substituindo na equação obtemos

$$\phi^3 + 1 = 2(\phi^2 - 1)^2 \Leftrightarrow \phi(\phi + 1) + 1 = 2\phi^2 \Leftrightarrow 1 + \phi = \phi^2,$$

o que é verdade.

Se G é um diamante, então podemos supor sem perda de generalidade que G_1 é também um diamante (e_1 é uma aresta já existente em G) e G_2 é um K_4. Nesse caso, como já feito antes

$$P_G(\lambda) = P_{G_1}(\lambda) = \lambda(\lambda - 1)(\lambda - 2)^2.$$

E pelo exemplo 3.5 temos que

$$P_{G_2}(\lambda) = \lambda(\lambda-1)(\lambda-2)(\lambda-3)$$

Calculando e usando que $\phi^2 = \phi + 1$ nós obtemos

$$\begin{aligned} P_G(\phi+1) = (\phi+1)(P_{G_1}(\phi+1) + P_{G_2}(\phi+1)) \Leftrightarrow \\ (\phi+1)\phi(\phi-1)^2 = (\phi+1)((\phi+1)\phi(\phi-1)^2 + (\phi+1)\phi(\phi-1)(\phi-2)) \Leftrightarrow \\ (\phi-1) = (\phi+1)(\phi-1) + (\phi+1)(\phi-2) \Leftrightarrow \\ \phi - 1 = (\phi^2-1) + (\phi^2-\phi-2) \Leftrightarrow 2(\phi^2-\phi-1) = 0 \end{aligned}$$

o que é verdade.

O último caso base é quando G consiste de um dos casos anteriores mais alguns vértices isolados. Neste caso basta usar que o polinômio cromático de G é o produto dos polinômios cromáticos de suas componentes. Como todas as componentes exceto uma são vértices isolados, então esse caso é o mesmo que os anteriores com um fator ϕ^{n-4} multiplicado.

Agora suponha que queremos provar pra G e G é um grafo em que existe pelo menos uma aresta a mais além das arestas nos vértices de F. Seja e essa aresta. Então $G-e$ e G/e ambos possuem a face quadrilateral F. Assim fazendo $G' = G-e$, $G'_i = G' + e_i$, $i = 1,2$ e $G'' = G/e$, $G''_i = G'' + e_i$, $i = 1,2$ temos por hipótese de indução que

$$\begin{aligned} P_{G'}(\phi+1) = (\phi+1)(P_{G'_1}(\phi+1) + P_{G'_2}(\phi+1)) \\ P_{G''}(\phi+1) = (\phi+1)(P_{G''_1}(\phi+1) + P_{G''_2}(\phi+1)). \end{aligned}$$

Como a aresta retirada nao continha as duas extremidades em F segue que $G_i - e = G'_i$ e $G_i/e = G''_i$ para $i = 1,2$. Logo subtraindo as duas equações acima e usando a Proposição 3.4 temos

$$\begin{aligned} P_G(\phi+1) = P_{G'}(\phi+1) - P_{G''}(\phi+1) = (\phi+1)((P_{G'_1}(\phi+1) - P_{G''_1}(\phi+1)) + (P_{G'_2}(\phi+1) - P_{G''_2}(\phi+1))) \\ = (\phi+1)(P_{G_1}(\phi+1) + P_{G_2}(\phi+1)) \end{aligned}$$

□

O próximo lema é a essencia do Teorema.

Lema 3.18. *Se G é uma triangulação planar de n vértices, então $P_G(\phi+2) = (\phi+2)\phi^{3n-10}P_G^2(\phi+1)$.*

Demonstração. Primeiro suponha a configuração do lema anterior. Seja H um grafo planar de n vértices com uma face quadriláteral F e sejam e_1, e_2 as diagonais de F (podendo sim alguma dessas diagonais já existirem em H). Considere $H_i = H + e_i$, $i = 1,2$. Vamos mostrar que se a igualdade $P_G(\phi+2) = (\phi+2)\phi^{3v(G)-10}P_G^2(\phi+1)$ é verdadeira para $G = H_2, H_1/e_1, H_2/e_2$, então também vale para $G = H_1$.

Para isso note pelo lema anterior e Proposição 3.4 que

$$\begin{aligned} (P_{H_1}(\phi+1) + P_{H_1/e_1}(\phi+1)) + (P_{H_2}(\phi+1) + P_{H_2/e_2}(\phi+1)) = P_{H_1-e_1}(\phi+1) + P_{H_2-e_2}(\phi+1) = \\ 2P_H(\phi+1) = 2(\phi+1)(P_{H_1}(\phi+1) + P_{H_2}(\phi+1)). \end{aligned}$$

Assim vale que

$$P_{H_1/e_1}(\phi+1) + P_{H_2/e_2}(\phi+1) = (2\phi+1)(P_{H_1}(\phi+1) + P_{H_2}(\phi+1)) = \phi^3(P_{H_1}(\phi+1) + P_{H_2}(\phi+1)).$$

pois utilizando que $\phi^2 = \phi + 1$ temos que $\phi^3 = \phi(\phi+1) = \phi^2 + \phi = 2\phi + 1$. Agora Lema 3.17.ii nos fornece que

$$P_{H_2/e_2}(\phi+1) - P_{H_1/e_1}(\phi+1) = P_{H_1}(\phi+1) - P_{H_2}(\phi+1).$$

Multiplicando essas duas igualdades obtemos

$$P^2_{H_2/e_2}(\phi+1) - P^2_{H_1/e_1}(\phi+1) = \phi^3(P^2_{H_1}(\phi+1) - P^2_{H_2}(\phi+1)).$$

Ou reescrevendo

$$\phi^3 P^2_{H_1}(\phi+1) = P^2_{H_2/e_2}(\phi+1) - P^2_{H_1/e_1}(\phi+1) + \phi^3 P^2_{H_2}(\phi+1).$$

Multiplicando a equação por $(\phi+2)\phi^{3(n-1)-10}$ e usando que a igualdade do enunciado vale para $H_2, H_1/e_1, H_2/e_2$ temos

$$(\phi+2)\phi^{3n-10}P^2_{H_1}(\phi+1) = (\phi+2)\phi^{3(n-1)-10}P^2_{H_2/e_2}(\phi+1) - (\phi+2)\phi^{3(n-1)-10}P^2_{H_1/e_1}(\phi+1) +$$
$$(\phi+2)\phi^{3n-10}P^2_{H_2}(\phi+1) = P_{H_2/e_2}(\phi+2) - P_{H_1/e_1}(\phi+2) + P_{H_2}(\phi+2) = P_{H_1}(\phi+2)$$

e logo a igualdade também vale para H_1.

Agora considere todas as triangulações em que a igualdade acima não é satisfeita. Seja G a configuração que viola a igualdade com o menor número de vértices e que maximiza o grau máximo, ou seja, de todas as triangulações de tamanho mínimo que violam a igualdade G é a que possui maior grau. Seja x um vértice de maior grau em G. Vamos mostrar que todas as faces de G são adjacentes a x.

Relembre que em uma triangulação toda face é um triângulo. Porque toda a aresta está em pelo menos uma face, segue que para todo vértice não isolado existe um triângulo adjacente a ele. Seja xyz um triângulo adjacente a x. Suponha agora que exista uma outra face $x'yz$ compartilhando yz não adjacente a x. Vamos mostrar que $x = x'$. Como toda triangulação é conexa (todas as faces incluindo a externa são triângulos), disso seguirá que todas as faces são adjacentes a x.

Para notar isso tome $e_1 = \{x, x'\}$, $e_2 = \{y, z\}$, $H = G - \{yz\}$, $H_i = H + e_i$. Primeiro note que H_2 é uma triangulação onde $d_{H_2}(x) = d_G(x) + 1$, logo pela escolha de G segue que H_2 satisfaz a igualdade. É fácil ver também que H_1/e_1 e H_2/e_2 são triangulações e assim pela minimalidade de G esses dois grafos também satisfazem a igualdade. Portanto pela discussão anterior o grafo $H_1 = G$ também satisfaz a igualdade, o que contradiz a suposição sobre G. Logo $x = x'$.

Agora considere o grafo $G - x$. Do fato de todas as faces de G serem adjacentes a x temos que $G - x$ é livre de ciclos. Do fato que G é uma triangulação também temos que $G - x$ é conexo. Logo $G - x$ é uma árvore. Assim pelo Exemplo 3.6 temos

$$P_{G-x}(\lambda) = \lambda(\lambda-1)^{n-2}.$$

Como todas as faces são adjacentes a x, também segue que x é adjacente a todos os vértices de G. Logo fixando uma cor para x não podemos usar mais ela no restante do grafo. Daí

$$P_G(\lambda) = \lambda P_{G-x}(\lambda-1) = \lambda(\lambda-1)(\lambda-2)^{n-2}.$$

Usando que $\phi^2 = \phi + 1$ segue que

$$P_G(\phi+2) = (\phi+2)(\phi+1)\phi^{n-2} = (\phi+2)\phi^n.$$

Por outro lado temos que

$$(\phi+2)\phi^{3n-10}P^2_G(\phi+1) = (\phi+2)\phi^{3n-10}(\phi+1)^2\phi^2(\phi-1)^{2n-4}.$$

Como $\phi^2 = \phi + 1$ segue que $\phi - 1 = 1/\phi$ e daí

$$(\phi+2)\phi^{3n-10}P^2_G(\phi+1) = (\phi+2)\phi^{3n-10}(\phi+1)^2\phi^2\left(\frac{1}{\phi}\right)^{2n-4} = (\phi+2)(\phi+1)^2\phi^{n-4} = (\phi+2)\phi^n.$$

Logo segue que G satisfaz a igualdade, uma contradição. □

A demonstração sai agora de uma indução.

Demonstração do Teorema 3.14. Façamos indução no número de vértices de um grafo da seguinte forma. O nosso caso base será quando G é uma triangulação. Neste caso pelo Lema 3.18 temos que $P_G(\phi+2) = (\phi+2)\phi^{3n-10}P^2_G(\phi+1)$. Daí segue que $P_G(\phi+2) > 0$ se, e somente se, $P_G(\phi+1) \neq 0$. Isso é verdade pelo Lema 3.16, que nos diz que $\phi + 1$ nunca é raiz de um polinômio cromático.

Agora suponha que estamos lidando com um grafo G planar qualquer. Suponha por hipótese de indução que o teorema é verdadeiro para qualquer grafo H planar com menos vértices de G e para

qualquer grafo planar H com $v(H) = v(G)$ em que $G \subset H$. Fazer a indução desse jeito faz sentido, porque para qualquer grafo planar G podemos adicionar arestas até obtermos uma triangulação. Como G não é uma triangulação, existe uma face F com pelo menos 4 vértices. Seja e uma diagonal dessa face F que não está no grafo G. Considere $H = G + e$. Assim por hipótese de indução temos que $P_H(\phi + 2) > 0$ e $P_{H/e}(\phi + 2) > 0$. Logo pela Proposição 3.4

$$P_G(\phi + 2) = P_{H-e}(\phi + 2) = P_H(\phi + 2) + P_{H/e}(\phi + 2) > 0.$$

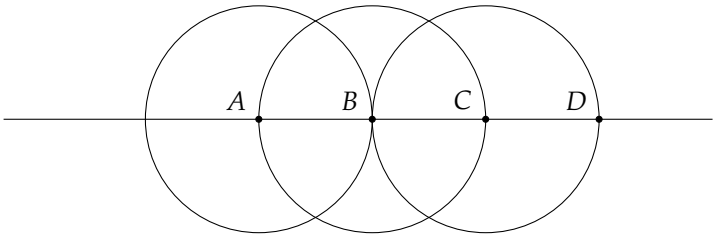
□

4 Construções com Régua e Compasso

◇ ◇ ◇ *Aula 9 (07 de Novembro) — Marcelo Campos* ◇ ◇ ◇

Nessa seção lidaremos com o problema de determinar quais distâncias são construtíveis com régua e compasso. Primeiro precisamos definir o jogo. Dizemos que uma distância é *construtível* com régua e compasso se é possível obter essa distãncia usando operações com régua em compasso em cima de uma distância inicial fixa de tamanho 1. Para exemplificar vamos mostrar que 3 é construtível.

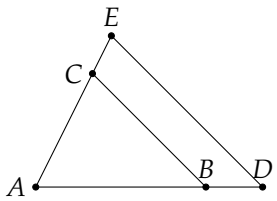
Usando da régua, trace uma reta s arbitrária no plano. Marque um ponto A nessa reta. O compasso nos permite medir distãncias, então abra o compasso com a medida fixa de tamanho 1. Isso significa que esse compasso é capaz de desenhar circumferências de raio 1 a partir de qualquer ponto. Escolha A como centro e seja B um dos pontos de intersecção da reta s com essa circumferência. Agora continuando o processo, trace outra circumferência com centro agora B e seja C o ponto de intersecção dela com a reta s (ponto distinto de A). Por fim faça esse processo mais uma vez obtendo o ponto D. O segmento AD construído tem tamanho 3, o que prova que 3 é construtível.



A operação descrita acima é chamada de *concatenação*. Basicamente uma concatenação une dois segmentos para formar um próximo. No nosso caso nós unimos três segmentos de tamanho 1 para obtermos um segmento de tamanho 3. Mas é fácil ver que isso também seria possível se os segmentos tivessem tamanho distintos (nesse caso teríamos que alterar o tamanho das circumferências). Com concatenação podemos concluir que todos os inteiros positivos são construtíveis. Além disso podemos concluir por concatenação que se as distâncias α, β são construtíveis, então $\alpha + \beta$ é construtível.

Podemos estender esses conceitos para números negativos. Como fazemos isso? Podemos interpretar o jogo da seguinte forma. Suponha que temos a reta real e nos foi dado o ponto 0 e o pontos 1. Quais pontos reais é possível determinar nessa reta? Note que esse problema é exatamente o mesmo de determinar quais são as distâncias construtíveis, pois para determinar um ponto α nessa reta com régua e compasso nós precisamos determinar a distâncial $|\alpha|$. Dizemos que um número real é *construtível* se ele pode ser determinado na reta real, onde é apenas nos dado o 0 e o 1, com uma série de construções com régua e compasso no plano euclideano. A concatenação do parágrafo anterior nos permite dizer que todos os inteiros são construtíveis. Além disso é fácil ver disso também que se α, β são construtíveis, então $\alpha \pm \beta$ é construtível.

Porém também é possível construir todos os elementos de $\mathbb{Q}$. Isso é possível devido ao Teorema de Tales. Seja $q = \frac{a}{b}$ um racional positivo qualquer. Uma propriedade lúdica de construções com régua e compasso é que dado uma reta s e um ponto P fora dela, é possível construir uma reta r paralela a s tal que $P \in r$. Assim podemos construir q como na próxima figura.



Construa segmentos AB e AC de tamanho b e a, respectivamente. Agora estenda AB até um ponto D tal que BD tenha tamanho 1 (lembre que possuimos a distância 1). Podemos construir uma paralela a BC passando por D. Essa paralela intersecta a reta AC em um ponto E. Pelo Teorema de Tales é possível determinar a distância CE. De fato

$$\frac{AB}{BD} = \frac{AC}{CE} \Leftrightarrow \frac{b}{1} = \frac{a}{CE} \Leftrightarrow CE = \frac{a}{b}.$$

Como sabemos construir todos os inteiros, inclusive a e b, essa construção nos mostra que todos os racionais são construtíveis. Além disso, ela mostra que se α, β são construtíveis, então α/β é construtível. Se trocarmos $AB = 1$ e $BD = \beta$ obtemos dessa mesma construção que se α, β são construtíveis, então $\alpha\beta$ é construtível.

A última observação nos permite concluir que o conjunto de pontos construtíveis é na verdade um corpo, pois é fechado em soma e multiplicação. Antes de continuarmos vamos estudar um pouco mais sobre corpos. Dado dois corpos E, F com $E \subset F$ nós podemos considerar F como um espaço vetorial em E. Tendo isso em vista, é natural perguntarmos qual a dimensão de F sobre E. Definimos $[F : E]$ como a dimensão de F como espaço vetorial de E. Se F tem dimensão infinita, então $[F : E] = \infty$. Além disso dizemos que F é uma extensão de E.

Um exemplo simples de extensão de um corpo E é a extensão $E(\alpha)$ onde $\alpha \notin E$. Definimos $E(\alpha)$ como o menor corpo contendo E e α. É possivel ver que isso é equivalente a dizer que

$$E(\alpha) = \{\frac{a_0 + a_1\alpha + \ldots + a_r\alpha^r}{b_0 + b_1\alpha + \ldots + b_s\alpha^s} : r, s \in \mathbb{N}, a_0, \ldots, a_r, b_0, \ldots, b_s \in E\}$$

O proximo lema nos diz que se α é raiz de um polinômio em $E[x]$, então é possível determinar a dimensão de $E(\alpha)$ como espaço vetorial de E.

Lema 4.1. *Seja E um corpo, $\alpha \in \overline{E}$ algébrico. Seja $p \in E[x]$ o polinômio mônico de grau mínimo tal que $p(\alpha) = 0$. Então $[E(\alpha) : E] = deg(p)$.*

Demonstração. Considere o conjunto

$$F = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} : a_0, \ldots, a_{n-1} \in E\},$$

onde $n = deg(p)$. Vamos mostrar que $F = E(\alpha)$. Primeiro note que como F é gerado por combinações lineares de potência de α, então $F \subset E(\alpha)$. Como $E(\alpha)$ é o menor corpo contendo E e α e F contém E e α segue então que basta mostrar que F é um corpo.

Existe uma aplicação natural sobrejetiva $\phi : E[x] \to F$ dada por

$$\phi(f) = f(\alpha).$$

De fato, dado $f \in E[x]$ qualquer, pelo algoritmo da divisão euclideana temos que existem q, r com $deg(r) < deg(p)$ tal que $f = pq + r$. Aplicando α nós obtemos

$$f(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = r(\alpha).$$

Isso significa que $\phi(f) = r(\alpha)$ onde r possui grau menor que $deg(p) = n$. Isso mostra que a aplicação possui como imagem F. É óbvio que ϕ é sobrejetiva. Além disso é fácil conferir que ϕ é um homomorfismo. Como $E[x]$ é um anel, segue que F também é.

Para mostrarmos que F é um corpo basta mostrarmos que um elemento $a \in F$ possui inverso, isto é, $a^{-1} \in F$. Vamos mostrar que se $f \in E[x]$, então $1/f(\alpha) \in F$. Usando que ϕ é sobrejetiva o resultado segue. Façamos isso por indução no grau de f. Se $deg(f) = 0$, então f é constante e logo $1/f(\alpha) \in E \subset F$.

Se $deg(f) > 0$, então pela divisão euclideana existem q, r com $deg(r) < deg(f)$ tal que $p = fq + r$. Assim

$$f(\alpha)q(\alpha) + r(\alpha) = p(\alpha) = 0 \Leftrightarrow \frac{1}{f(\alpha)} = -\frac{q(\alpha)}{r(\alpha)}.$$

Por hipótese de indução temos que $1/r(\alpha) \in F$ e como F é um anel segue que $1/f(\alpha) \in F$.

Agora note que $1, \alpha, \ldots, \alpha^{n-1}$ é uma base de F como espaço vetorial em E. Isso ocorre pois caso contrário teríamos uma combinação linear $c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1} = 0$ e em particular α seria raiz do polinômio $g(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$, o que contradiz a minimalidade de p. Assim F tem dimensão n como espaço vetorial de E e dai $[E(\alpha) : E] = n = deg(p)$. □

O próximo lema nos diz que as dimensões de uma torre de extensões de corpos se comportam bem.

Lema 4.2. *Sejam $E \subset F \subset K$ corpos. Então $[K : E] = [K : F][F : E]$.*

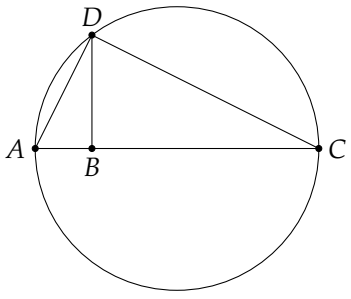
Demonstração. Seja $\{u_1, \ldots, u_n\}$ uma base de F como espaço vetorial em E e $\{v_1, \ldots, v_m\}$ uma base de K como espaço vetorial em E. Afirmamos então que $\{u_iv_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ é uma base de K como espaço vetorial em E e consequentemente que $[K : E] = [K : F][F : E]$.

Seja $x \in K$, podemos escrever $x = \sum_{j=1}^{m} b_jv_j$ com $b_j \in F$. Agora para cada j podemos escrever $b_j = \sum_{i=1}^{n} a_{ij}u_i$. Juntando tudo obtemos que $x = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}u_iv_j$. Isso prova que $\{u_iv_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ gera K. Vamos ver agora que esse conjunto é linearmente independente. Suponha que $\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}u_iv_j = 0$. Podemos reescrever isso como $\sum_{j=1}^{m} d_jv_j = 0$, onde $d_j = \sum_{i=1}^{n} c_{ij}u_i \in F$. Como v_j's são linearmente independentes segue que $d_j = 0$ para todo j, isto é, $\sum_{i=1}^{n} c_{ij}u_i = 0$ para todo $1 \leq j \leq m$. Mas agora a independência linear em u_i nos dá que $c_{ij} = 0$ para todo i, j. □

Retornando ao problema de construções com régua e compasso, suponha que sabemos construir todos os números em um corp $F \subset R$. Isso implica que dados os eixos e o ponto $(0, 0)$ do plano cartesiano nós sabemos determinar todos os pontos de $F^2 \subset \mathbb{R}^2$. Agora observe que construções com régua e compasso utilizam de basicamente três operações: Marcar pontos, traçar retas e traçar circulos de determinado raio. Queremos construir pontos novos no plano, que em última instância significariam distâcias novas. Suponha que seja possível construir um ponto novo. Para construir esse ponto podemos supor sem perda que todos os pontos marcado, retas traçadas e circulos desenhados estão em F. A razão para qual podemos supor isso é porque essas são as unicas retas, circulos e pontos que sabemos determinar. Qualquer outra opção seria um chute e logo, como é um chute, a gente pode supor que é um dos casos anteriores.

Isso basicamente significa que todas as retas são da forma $ax + by + c = 0$ com $a, b, c \in F$ e todos os círculos são da forma $(x - a)^2 + (y - b)^2 = c^2$ com $a, b, c \in F$. O ponto novo será obtidos por intersecções dessas retas e círculos. É fácil ver que a intersecção de duas retas em F nos dará um ponto em F^2. Agora a intersecção de uma reta em F com um círculo em F nos dará no pior dos casos um ponto de coordenadas em $F(\sqrt{a})$ para algum $a \in F$, pois precisamos resolver uma equação quadrática. O mesmo pode ser obtido por intersecções de dois círculos. Isso nos permite concluir que qualquer ponto construido novo é um elemento de $F(\sqrt{a})$ para algum $a \in F$ e se tivermos uma nova distância, ela seria um elemento de $F(\sqrt{a})$.

Porém note que $\sqrt{a}$ é construtível. Para isso considere a construção como na figura abaixo. Seja AC um segmento de tamanho $a + 1$, dividido em dois segmentos AB e AC de tamanhos 1 e a, respectivamente. Construa uma circunferência de diâmetro AC e seja D a intersecção da perpendicular a AC passando por B com a circunferência.



Por semelhança de triângulos temos

$$\frac{AB}{BD} = \frac{BD}{BC} \Leftrightarrow \frac{1}{BD} = \frac{BD}{a} \Leftrightarrow BD = \sqrt{a}.$$

Como inicialmente sabemos construir o $\mathbb{Q}$ isso permite caracterizar os reais construtíveis da seguinte forma. Um número α é construtível se, e somente se, existe um inteiro n e uma sequência de corpos $\mathbb{Q} = K_1 \subset \ldots \subset K_n$ tais que $\alpha \in K_n$ e $[K_{i+1} : K_i] = 2$ para todo $1 \leq i \leq n-1$. Isso acontece porque obviamente pelo Lema 4.1 temos que $[F(\sqrt{a}) : F] = 2$, se $\sqrt{a} \notin F$. A partir de agora vamos usar essa caracterização como a definição de um número construtível. A vantagem é que essa definição nos permite estender números construtíveis para números complexos.

Uma outra consequência dessa observação e do Lema 4.2 é que todo número construtível é elemento de um corpo K tal que $[K : \mathbb{Q}] = 2^n$ para algum n. Isso nos permite provar alguns resultados sobre construções com régua e compasso. Antes um resultado preliminar importante.

Teorema 4.3. *Seja $p(x) = x^3 + a_2x^2 + a_1x + a_0$ um polinômio irredutível em $\mathbb{Q}[x]$. Entao as raízes de p não são construtíveis.*

Demonstração. Seja α uma raiz de p. Seja f o polinômio mônico de menor grau em $\mathbb{Q}[x]$ tal que α é raiz. Pelo algoritmo de divisão euclideana existe $q, r \in \mathbb{Q}[x]$ com $deg(r) < deg(f)$ tal que $p = fq + r$. Porém aplicando essa igualdade em α obtemos que $r(\alpha) = 0$. Pela minimalidade de f concluimos que r é identicamente nulo e portanto $p = fq$. Usando que p é irredutível e também mônico, segue que $q \equiv 1$ e daí $f = p$. Aplicando o Lema 4.1 temos que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Se α fosse construtível existiria um corpo K tal que $\alpha \in K$ e $[K : \mathbb{Q}] = 2^n$. É fácil ver das propriedades de corpos que $\mathbb{Q}(\alpha) \subset K$. Portanto pelo Lema 4.2 nós temos que $2^n = [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 3[K : \mathbb{Q}(\alpha)]$. Logo $3 \mid 2^n$, o que é impossivel. Portanto α não é construtível. □

Como aplicação de tudo que foi estudado aqui vamos resolver um problema clássico em construções de régua e compasso. Dado um ângulo, é possível por meios engenhosos encontrar a bissetriz desse ângulo. Isso nos permite obter metade de um ângulo para qualquer ângulo dado. A pergunta natural é se é possível triseccionar um ângulo, ou seja, obter um terço de um ângulo. Esse problema é muito antigo, proposto provavelmete ainda na grécia antiga, que só foi resolvido com as técnicas apresentadas nesta aula.

Teorema 4.4. *É impossível triseccionar um ângulo com régua e compasso.*

Demonstração. Para provarmos que é impossível, vamos na verdade resolver outro problema. Vamos mostrar que é impossível construir um ângulo de 20^o com régua e compasso. Note que construir um ângulo γ é equivalente a construir $\cos\gamma$. De fato, considere a circunferência de raio 1 na origem do plano cartesiano. Se soubermos construir o ângulo γ, então construindo ele no sentido anti-horário na circunferência é suficiente para obter um triângulo retângulo com lados $\cos\gamma$ e $\sin\gamma$. Se tivermos a medida $\cos\gamma$ então basta traçar a paralela a reta $y = 0$ passando pelo ponto $(\cos\gamma, 0)$ e considerar sua intersecção com a circunferência. Assim queremos mostrar que $\cos 20^o$ é construtível.

Seja $\omega = e^{\gamma i}$. Um cálculo nos mostra que

$$(2\cos\gamma)^3 = (\omega + \omega^{-1})^3 = \omega^3 + 3\omega + 3\omega^{-1} + \omega^{-3} = 2cos3\gamma + 6cos\gamma$$

Substituindo $\gamma = 20^o$ obtemos

$$(2\cos(20^o))^3 - 3(2\cos(20^o)) - 1 = 0.$$

Isso significa que $\alpha = 2\cos(20^o)$ é raiz do polinômio $p(x) = x^3 - 3x - 1$. Porém uma análise simples mostra que $p(x)$ não possui raizes racionais. Assim pelo Teorema 4.3 temos que α não é construtível e logo $\cos(20^o)$ também não é.

Agora suponha que exista um algoritmo para triseccionar um ângulo. Então nesse caso poderíamos construir o ângulo de 20^o. Isso ocorre porque é possível construir o ângulo de 60^o. De fato, o número $\cos 60^o$ está em $\mathbb{Q}[\sqrt{3}]$ e logo é construtível. Construindo esse ângulo e triseccionando ele obtemos o ângulo desejado, o que é uma contradição. □

◇ ◇ ◇ *Aula 10 (14 de Novembro) — Marcelo Campos* ◇ ◇ ◇

Dizemos que um polígono regular é construtível se podemos construir ele usando apenas régua e compasso. Vamos mostrar o seguinte teorema sobre construtibilidade de polígonos regulares. Um primo p é um primo de Fermat se $p = 2^{2^t} + 1$ para algum $t \geq 0$ inteiro.

Teorema 4.5. *Se um n-ágono regular é construtível, então $n = 2^r p_1 \dots p_s$, onde os p_i's são primos de Fermat distintos.*

Para provarmos esse teorema vamos precisar usar as técnicas da aula anterior. A técnica consiste em reduzir um problema de construção com régua e compasso em determinar se um número α é construtível. Nós sabemos que se um número é construtível, então ele está contido em um corpo K tal que $[K : \mathbb{Q}] = 2^n$. Assim para provarmos que esse número não é construtível basta mostrarmos pelo Lema 4.2 que $[\mathbb{Q}(\alpha) : Q]$ contém um fator diferente de 2. O Lema 4.1 nos mostra que para entendermos essa dimensão, nós precisamos conhecer o polinômio minimal de α. Para o Teorema 4.5 o polinômio em particular que será estudado é o polinômio ciclotômico.

O n-ésimo polinômio ciclotomico $\Phi_n(x)$ é um polinômio de coeficientes racionais definido como o fator de $x^n - 1$ que não divide $x^k - 1$ para todo $k < n$. Uma maneira equivalente de definir seria pela seguinte recursão

$$\Phi_1(x) = x - 1,$$
$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n} \Phi_d(x)}, \quad \forall n > 1.$$

Para nossos intuitos nós vamos precisar do próximo teorema que será enunciado sem demonstração.

Teorema 4.6. *O polinômio ciclotomico $\Phi_n(x)$ é mônico, de coeficientes inteiros e irredutível em $\mathbb{Q}$. Além disso*

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ mdc(k,n)=1}} (x - e^{2\pi i \frac{k}{n}})$$

Esse último teorema nos diz que $e^{\frac{2\pi i}{n}}$ é raiz de $\Phi_n(x)$ e como o polinômio é irredutível e mônico, temos que $\Phi_n(x)$ é o seu polinômio minimal (vide demonstração do Teorema 4.3). Além disso o teorema nos mostra que $deg(\Phi_n) = \varphi(n)$. Assim podemos aplicar o Lema 4.1 para concluir o seguinte corolário.

Corolário 4.7. *Seja n inteiro. Então $[\mathbb{Q}(e^{\frac{2\pi i}{n}}) : \mathbb{Q}] = \varphi(n)$.*

Veremos agora como isso é suficiente.

Demonstração do Teorema 4.5. Suponha que para determinado n é possível construir um n-ágono regular. Isso signfica em particular que conseguimos contruir todos os ângulos internos do polígono, ou seja, que conseguimos construir o ângulo de $\frac{n-2}{n}\pi$. Se isso é possível, então mediante a uma reta conseguimos construir também o ângulo de $\pi - \frac{n-2}{n}\pi = \frac{2\pi}{n}$. Como já vimos antes, isso é equivalente a dizer que $\cos(\frac{2\pi}{n})$ é construtível.

Seja $\omega = e^{\frac{2\pi i}{n}}$. Note então que $\cos(\frac{2\pi}{n}) = \frac{\omega+\omega^{-1}}{2} \in \mathbb{Q}(\omega + \omega^{-1})$. Como $\omega + \omega^{-1} \in \mathbb{Q}(\omega)$, segue que $\mathbb{Q}(\omega + \omega^{-1})$ é um corpo intermediário entre $\mathbb{Q}$ e $\mathbb{Q}(\omega)$. Vamos mostrar que $[\mathbb{Q}(\omega) : \mathbb{Q}(\omega + \omega^{-1})] \mid 2$. De fato, isso segue do Lema 4.1 observando que ω é uma raiz do polinômio $p(x) = x^2 - (\omega + \omega^{-1})x + 1 \in \mathbb{Q}(\omega + \omega^{-1})[x]$. Se $p(x)$ for o polinômio minimal, então segue do lema que $[\mathbb{Q}(\omega) : \mathbb{Q}(\omega + \omega^{-1})] = 2$. Caso contrário, então o polinômio minimal tem grau 1, o que significa que $\mathbb{Q}(\omega) = \mathbb{Q}(\omega + \omega^{-1})$ e $[\mathbb{Q}(\omega) : \mathbb{Q}(\omega + \omega^{-1})] = 1$.

Agora usando o Corolário 4.7 obtemos que $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$ e logo $[\mathbb{Q}(\omega + \omega^{-1}) : \mathbb{Q}] \in \{\phi(n)/2, \phi(n)\}$. Como já discutido, para que $\cos(\frac{2\pi}{n})$ seja construtível, temos que ter $[\mathbb{Q}(\omega + \omega^{-1}) : \mathbb{Q}] \mid 2^m$ para algum $m \geq 0$. Isso significa que $\phi(n) \mid 2^m$ para algum $m \geq 0$, ou seja, $\phi(n)$ é uma potência de 2.

Se $n = p$ primo ímpar, então segue que $\phi(p) = p - 1 = 2^m$ para algum $m \geq 0$. Isto é, p é um primo da forma $2^m + 1$. É possível ver neste caso que devemos ter m como potência de 2. Suponha o contrário, que $m = qk$ onde q é um primo ímpar. Então podemos escrever

$$2^m + 1 = 2^{qk} + 1 = (2^k + 1)((2^k)^{q-1} - (2^k)^{q-2} + \dots - (2^k) + 1)$$

e como os dois fatores são diferentes de 1, isso contradiz $2^m + 1$ ser primo. Logo m não possui fatores ímpares e é uma potência de 2. Isso significa que para ser construtível devemos ter p primo de Fermat.

Agora suponha que $n = p^2$, onde p é primo ímpar. Então para esse caso temos que $\phi(n) = p(p-1) = 2^m$ para algum inteiro $m \geq 0$. Porém isso implica que $p \mid 2^m$, o que é impossível para um primo ímpar. A conclusão então é que nenhum polígono regular de p^2 lados é construtível.

Para finalizar note que se é possível construir um nm-ágono regular, então em particular é possível construir um m-ágono regular e um n-ágono regular. Assim todos se um n-ágono regular é construtível, então todos polígonos regulares com número de lados divisor de n tem de ser construtíveis. Isso implica pelos parágrafos anteriores que todos os fatores primos de n são primos de Fermat e que não existe primo ímpar p tal que $p^2 \mid n$. Logo podemos concluir o enunciado. □

É interessante observar que a volta do Teorema 4.5 também é verdadeira, isto é, todo n-ágono regular com $n = 2^s p_1 \dots p_r$ e p_i's primos de Fermat é construtível. Porém não iremos demonstrar esse resultado.

Estudamos um pouco o caso de extensões de corpos de dimensão finita. Vimos que extensões geradas por raizes de polinômios irredutiveis em $\mathbb{Q}$ são finitas. É fácil ver que em uma extensão finita F de E, todo elemento de F é raíz de um polinômio em E. De fato, para $\alpha \in F$, basta considerar $1, \alpha, \alpha^2, \dots$. Como a dimensão de F é finita, esses números são linearmente dependentes e existe uma combinação linear finita que soma 0. Essa combinação linear nos dá um polinômio em E como desejado. Isso permite definir o conceito de número algébrico. Dizemos que α é algébrico sobre E se α é raiz de um polinômio em E. A discussão acima basicamente nos diz que toda extensão finita de E só possui elementos algébricos em E.

Porém o que acontece quando α não é raíz de nenhum polinômio em E? Nesse caso então a extensão $E(\alpha)$ possuirá dimensão infinita, o que é particularmente interessante. Dizemos que um α é trascedental em E se α não é raíz de nenhum polinômio com coeficientes em E. É um resultado clássico em álgebra que existem números reais transcedentais (em $\mathbb{Q}$). Os exemplos mais famosos são os números e e π. Vamos provar aqui que e é trascedental.

Antes uma pequena observação. Para provarmos que e é transcedental, temos que provar que ele não é raiz de nenhum polinômio $p \in \mathbb{Q}[X]$. Note que isso na verdade é equivalente a mostrar que ele não é raiz de nenhum polinômio em $\mathbb{Z}[x]$. Isso vem do fato de que todo polinômio em $\mathbb{Q}[x]$ é um polinômio em $\mathbb{Z}[x]$ multiplicado por uma constante apropriada em $\mathbb{Q}$. Assim podemos assumir de agora em diante que estamos interessados em provar que e não é raiz de nenhum polinômio em $\mathbb{Z}[x]$.

Teorema 4.8. *O número e é transcedental.*

Demonstração. A prova é baseada na seguinte observação. Seja f uma função de classe C^∞, isto é, uma função infinitamente derivável bem comportada. Considere a seguinte espécie de transformada de Fourier de f

$$S(f, x) = \int_0^x f(t)e^{-t}\,\mathrm{d}t.$$

Usando integração por partes obtemos que

$$S(f, x) = \int_0^x f(t)e^{-t}\,\mathrm{d}t = \int_0^x f'(t)e^{-t}\,\mathrm{d}t - [f(t)e^{-t}]_0^x = S(f', x) - f(x)e^{-x} + f(0).$$

O que pode ser visto como uma espécie de recursão de f pela sua derivada f'. Somando essa útlima equação para $f, f', f'', \dots$ e fazendo

$$F(x) = \sum_{k=0}^{\infty} f^{(k)}(x)$$

temos que

$$\int_0^x F(t)e^{-t}\,\mathrm{d}t = \sum_{k=0}^{\infty} S(f^{(k)}, x) = \sum_{k=0}^{\infty} S(f^{(k+1)}, x) - F(x)e^{-x} + F(0) = \int_0^x (F(t) - f(t))e^{-t}\,\mathrm{d}t + F(0) - F(x)e^{-x}$$

e daí segue que

$$\int_0^x f(t)e^{-t}\,\mathrm{d}t = F(0) - F(x)e^{-x},$$

para todo $x \geq 0$.

Suponha que e seja um número algébrico. Isto é, suponha que existam $a_0, \ldots, a_n \in \mathbb{Z}$ e $a_0 \neq 0$ tais que

$$a_0 + a_1 e + \ldots + a_n e^n = 0.$$

Usando a igualdade do parágrafo acima de um jeito esperto obtemos

$$\sum_{k=0}^{n} a_k e^k \int_0^k f(t)e^{-t}\,\mathrm{d}t = F(0)\sum_{k=0}^{n} a_k e^k + \sum_{k=0}^{n} a_k F(k) = \sum_{k=0}^{n} a_k F(k).$$

Até agora não falamos nada sobre a função f. O plano é tomar f como um polinômio, isso garante que f é de classe C^∞ e que todas as operações feitas até agora (como trocar limites) estão corretas. A nossa escolha de f será de tal forma em que o lado direito da última equação seja inteiro não nulo, enquanto o lado esquerdo seja pequeno tendendo a zero. Ao fazermos isso obteremos uma contradição que implicará que e é transcedental.

O nosso polinômio será

$$f(x) = \frac{1}{(p-1)!}x^{p-1}(x-1)^p(x-2)^p\ldots(x-n)^p,$$

Onde p é um primo suficientemente grande. Primeiro vamos mostrar que com a escolha apropriada de p podemos garantir que o lado esquerdo da equação seja pequeno. De fato,

$$\Big|\sum_{k=0}^{n} a_k e^k \int_0^k f(t)e^{-t}\,\mathrm{d}t\Big| \leq \sum_{k=0}^{n} |a_k e^k| \frac{M}{(p-1)!},$$

onde $M = \max_{0\leq x\leq n}\{(p-1)!|f(x)|\}$. É fácil ver que $M \leq A^p$ onde $A = \max_{0\leq x\leq n}\{|x(x-1)\ldots(x-n)|\}$. De onde segue que

$$\Big|\sum_{k=0}^{n} a_k e^k \int_0^k f(t)e^{-t}\,\mathrm{d}t\Big| \leq \frac{A^p}{(p-1)!}\sum_{k=0}^{n} |a_k e^k| \to 0,$$

para p suficientemente grande, pois $(p-1)!$ cresce mais rápido do que exponencial. Em particular, existe uma escolha de p tal que o lado esquerdo em módulo é menor que $1/2$.

Agora vamos mostrar que o lado direito é inteiro para p suficientemente grande. Note que f é um polinômio de grau $pn + (p-1)$ em $\mathbb{Q}[x]$. Vamos mostrar que para $t \geq p$, $f^(t)(x)$ é um polinômio em $\mathbb{Z}[x]$ cujo todos os coeficientes são múltiplos de p. Isso vem do fato que podemos escrever f como

$$f(x) = c_0 + c_1 x + \ldots + c_s x^s,$$

onde $s = pn + (p-1)$. Daí

$$f^{(t)}(x) = \sum_{i=t}^{s} c_i i(i-1)\ldots(i-t+1)x^{i-t}.$$

Porém $c_i = \frac{b_i}{(p-1)!}$ onde $b_i \in \mathbb{Z}$. Então segue que

$$c_i i(i-1)\ldots(i-t+1) = b_i p\binom{i}{p}(i-p)\ldots(i-t+1),$$

inteiro mútliplo de p. Isso significa que $f^{(t)}(k)$ é inteiro e múltiplo de p para todo $t \geq p$ e $0 \leq k \leq n$.

Resta calcular quando $t < p$. Para isso divida em dois casos. Primeiro vamos lidar com $f^{(t)}(k)$ quando $k \neq 0$. Neste caso ao derivarmos t vezes usando a regra do produto, obteremos diversos termos, porém em todos o expoente do fator $(x-k)$ será pelo menos $p-t > 0$. Isso significa que k será uma raiz do polinômio e portanto $f^{(t)}(k) = 0$ para $t < p$ e $k \neq 0$. Agora suponha que $k = 0$. Novamente o mesmo pode ser aplicado aqui. Ao derivarmos t vezes utilizando a regra do produto, o fator x terá expoente pelo menos $p-1-t$ em todos os fatores. Se $p-1-t > 0$, isso significa que 0 é raiz e portanto $f^{(t)}(0) = 0$. Caso $t = p-1$, então existe um termo em que o fator x tem expoente 0. Esse termo é exatamente

$$\frac{(p-1)!}{(p-1)!}(x-1)^p \dots (x-n)^p = (x-1)^p \dots (x-n)^p.$$

Portanto temos que

$$f^{(p-1)} = (-1)^n n!,$$

que é inteiro.

Isso conclui que $F(k) = \sum_{i=0}^{\infty} f^{(i)}(k)$ é inteiro para todo $0 \leq k \leq n$. Além disso, os nossos cálculos mostrararm que

$$F(k) \equiv \begin{cases} (-1)^n n! \,(\mathrm{mod} p), & \text{se } k = 0 \\ 0 \,(\mathrm{mod} p), & \text{se } k \neq 0 \end{cases}.$$

Portanto temos que

$$\sum_{k=0}^{n} a_k F(k) \equiv a_0 (-1)^n n! \not\equiv 0 \,(\mathrm{mod} p),$$

se escolhermos $p > |a_0 n!|$. Daí concluimos que $\sum_{k=0}^{n} a_k F(k)$ é um inteiro não nulo e $\sum_{k=0}^{n} a_k e^k \int_0^k f(t) e^{-t} \, \mathrm{d}t$ tem valor absoluto menor do que 1/2, logo esses dois valores não podem ser iguais, o que é uma contradição. □