MAT-240 Diurno – Construções Geométricas - Resumo

Prof. Paulo Ferreira Leite

junho de 2008

1 Construções Geométricas

Um método eficiente de estudar as construções geométricas com instrumentos, como por exemplo, régua e compasso, um único desses instrumentos, ou ainda com a ajuda de curvas auxiliares, é formalizar os conceitos utilizados na construção de modo a estabelecer uma correspondência entre eles e as operações algébricas definidas em um corpo transformando assim os problemas de construção em problemas algébricos.

1.1 Pontos e Números Construtíveis

1. Vamos inicialmente definir formalmente construções com régua e compasso. Na definição que adotamos o compasso é o compasso euclidiano que serve para construir uma circunferência cujo centro é um ponto dado e que passa por um ponto dado. Esse compasso não pode ser utilizado para transportar segmentos.

   Seja Σ um subconjunto qualquer do plano com, pelo menos, dois elementos.

   Chamaremos de figuras associadas a Σ ou simplesmente figuras de Σ, retas que contenham, pelo menos, dois pontos de Σ e circunferências cujo centro, e pelo menos mais um ponto, estejam em Σ.

Diremos que um ponto é *imediatamente construtível* a partir de Σ se for determinado pela intersecção de duas figuras de Σ.

2. **Definição.** Dizemos que um ponto P é *construtível* se existir uma seqüência finita $P_1, P_2, \ldots, P_n = P$ de pontos tais que

   (a) P_1 é *imediatamente construtível* a partir de Σ

   (b) P_{i+1} é *imediatamente construtível* a partir de $\Sigma \cup \{P_1, P_2, \ldots, P_i\}$

3. **Definição.** Seja Σ um subconjunto do conjunto $\mathbb{R}$ dos números reais. Dizemos que um número real a é construtível a partir de Σ se a é a abscissa de um ponto do plano que é construtível a partir dos pontos da forma $(x, 0)$ com $x \in \Sigma$. No caso de números complexos, diremos que ele é construtível se suas partes reais e complexas o forem.

   A partir dessa definição, utilizando resultados simples de geometria podemos demonstrar

   Teorema 1 *Seja Σ um subconjunto dos números reais $\mathbb{R}$ que contem 0 e 1. Os números construtíveis a partir de Σ forma um subcorpo K_Σ de $\mathbb{R}$ que contem Σ e é estável por extração de raiz quadrada, isto é, se $a \in K_\Sigma$, então $\sqrt{a} \in K_\Sigma$*

4. O teorema básico para demonstrações de que determinados números não são construtíveis foi demonstrado por Wantzel (1814 - 1848) em 1837 e pode ser assim enunciado

   Teorema 2 *Seja K um subcorpo de $\mathbb{R}$. Uma condição necessária e suficiente para que um real a seja construtível a partir de K é que exista uma seqüência finita de subcorpos de $\mathbb{R}$ tal que*

   $$K \subset K_0 \subset K_1 \cdots \subset K_n$$

   com $[K_i : K_{i-1}] = 2$ *e* $a \in K_n$

Um corolário desse teorema, importante nas aplicações, afirma

Corolário Seja K um subcorpo de $I\!R$ e seja a um um número real construtível a partir de K. Então a é algebrico e seu grau sobre K é uma potência de 2.

5. Para podermos demonstrar o teorema de Wantzel e relacioná-lo com a definção de construtibilidade que demos acima vamos precisar fazer uma breve revisão de alguns fatos básicos de Álgebra relacionados com o estudo da extensão de corpos.

1.2 Aneis e Corpos - Revisão.

1. **Definição.** Dizemos que um corpo L é uma extensão do corpo K se K é um subcorpo de L.

   É muito fácil verificar que se L é uma extensão de K, então L admite uma estrutura de espaço vetorial sobre K. Verifique, como exercício, essa afirmação.

2. **Definição.** Dizemos que L é uma extensão finita de K se L, considerado como espaço vetorial sobre K, tem dimensão finita. Caso contrário, isto é, se essa dimensão não for finita dizemos que L é uma extensão infinita de K.

3. **Exemplos**

4. **Definição.** Seja L uma extensão do corpo K. Diz-se que um elemento α de L é algébrico sobre K se existe um polinômio $p(x)$ de $K[X]$ tal que $p(\alpha) = 0$. Se α não for algébrico diremos que α é transcendente sobre K. Se todos os elementos de L forem algébricos sobre K diremos que L é uma extensão algébrica de K. Se existir em L algum elemento não algébrico diremos que L é uma extensão não algébrica ou transcendente de K.

5. Veremos agora uma forma bastante útil de caracterizar os elementos algébricos e transcendentes de uma extensão de corpos. Seja L uma

extensão de K e x um elemento de L. Vamos associar a esse elemento x uma aplicação

$$\phi_x : K[X] \longrightarrow L$$

definida da seguinte maneira:

Dado o polinômio $P(X) \in K[X]$, colocamos, por definição,

$$\phi_x(P(X))(x) = a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n$$

Verifica-se sem dificuldade que essa aplicação é simultaneamente um homomorfismo de espaços vetoriais e de aneis. Portanto sua imagem alem de ser um subespaço vetorial de L é tambem um subanel do corpo L. Indicaremos esse subanel por $K[x]$ para indicar o fato de que ele é um subanel gerado por $K \cup \{x\}$. Veremos adiante que quando x é algébrico $K[x]$ é um corpo.

6. **Teorema 3** *Seja L uma extensão de K e x um elemento de L.*

   (a) *Se x é transcendente sobre E, ϕ_x é um isomorfismo e sua imagem $E[x]$ é um espaço vetorial de dimensão infinita.*

   (b) *Se x é algébrico sobre E, existe um único polinômio P de $K[X]$,mônico (o coeficiente do termo de maior grau é igual a 1) e de grau mínimo tal que $P(x) = 0$. Alem disso, P é irredutível e seu grau é igual a dimensão do espaço vetorial $K[x]$ sobre K. Qualquer outro polinômio de $K[X]$ que admita x como raiz é multiplo de P.*

   Esse teorema tem muitas conseguências importantes. Vamos mencionar apenas as que nos interessam mais de perto.

7. **Definição.** O polinômio P da proposição acima chama-se polinômio minimal de x sobre K. O grau de P chama-se grau de x sobre K. As outras raizes de P são chamadas de raizes conjugadas de x.

8. **Corolário 1** *Toda extensão finita de um corpo é uma extensão algébrica.*

9. **Teorema 4** *Seja L uma extensão de K e x e y elementos de L, algébricos sobre K. Nessas condições $x + y$ e xy são algébricos sobre K. Se $x \neq 0$, então $1/x$ tambem é algébrico sobre K e pertence a $K[x]$.*

10. **Corolário 2** *O conjunto dos elementos de L que são algébricos sobre K é um subcorpo de K.*

11. **Definição** Seja L uma extensão do corpo K. Chama-se grau da extensão à dimensão de E considerado como espaço vetorial sobre K. Indica-se o grau da extensão com o símbolo $[L : K]$.

12. **Teorema 5** *Suponha que L é uma extensão do corpo K e M é uma extensão do corpo L, então M é uma extensão finita de K se e somente se as extensões $K \subset L$ e $L \subset M$ são finitas. No caso das extensões serem finitas vale a formula*

$$[K : L][L : M] = [K : M]$$

13. **Teorema 6** *Considere as extensões $K \subset L$ e $L \subset M$. Se $x \in M$ é algébrico sobre L e L é uma extensão algébrica de K, então x é algébrico sobre K. Alem disso, se $K \subset L$ e $L \subset M$ são algébricas, então $K \subset M$ é algébrica.*

14. **Teorema 7** *Seja L uma extensão do corpo K e $x_1, x_2, \ldots, x_n$ elementos de L. As seguintes condições são equivalentes:*

    (a) os elementos $x_1, x_2, \ldots, x_n$ são algébricos sobre K

    (b) $K[x_1, x_2, \ldots, x_n]$ é de dimensão finita sobre K

    (c) $K[x_1, x_2, \ldots, x_n]$ é um corpo.

    (d) $K(x_1, x_2, \ldots, x_n)$é de dimensão finita sobre K

15. Divisão euclidiana de polinômios.

16. Seja $\mathbb{C}[X]$ o anel dos polinômios de uma variável sobre o corpo $\mathbb{C}$ dos números complexos.

17. **Teorema 8** *Todo polinômio* $p(z) \in \mathbb{C}[X]$ *de grau maior ou igual a um tem, pelo menos, uma raiz complexa.*

18. **Teorema 9** *Se o polinômio* $p(z) = a_o + a_1 z + \cdots + a_n z^n$ *tem todos os coeficientes inteiros e admite como raiz o número racional* r/s*, escrito em sua forma irredutível, (isto é, (m.d.c (r,s)=1), então* r *divide* a_o *e* s *divide* a_n