359 **A TEORIA DE SUBRESULTANTES APLICADA AO CÁLCULO DO MÁXIMO DIVISOR COMUM DE UM POLINÔMIO.** *Carlos Hoppen*, *Vilmar Trevisan* (Dept º de Matemática Pura e Aplicada, UFRGS).

Seja R um anel. Uma ferramenta básica da álgebra computacional é a divisão com resto, isto é, dados f, g $\in$ R, procuram-se q, r $\in$ R que satisfaçam: f = qg + r, r = 0 ou N(r) < N(g), onde N denota uma norma de R. Esse problema foi estudado pelo matemático grego Euclides (320-275 A. C.) para domínios euclideanos. Porém, dados f, g em um anel arbitrário, tais q e r nem sempre existem. Em particular, esse é o caso para polinômios em D[X], onde D é um domínio de integridade, o que motiva uma extensão para esse problema: para f, g $\in$ D[X], procuram-se α, β $\in$ D, q, r $\in$ D[X] tais que: αf = qg + βr e r = 0 ou grau(r) < grau(g). A solução desse problema e a determinação de pares (α, β) que otimizem a sua resolução computacional serão abordadas no trabalho seguindo o ponto de vista da Teoria de Subresultantes, cujo Teorema Fundamental motivará um algoritmo útil para determinar um elemento associado ao máximo divisor comum de dois polinômios quando os considerarmos sobre o corpo de frações de D. Resultados de complexidade e a comparação do desempenho de diferentes algoritmos para essa finalidade em exemplos concretos também serão apresentados. (Fapergs)