UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA APLICADA

Uma Generalização do Algoritmo de Gao para Fatoração de Polinômios

por

Carlos Hoppen

Dissertação submetida como requisito parcial
para a obtenção do grau de

Mestre em Matemática Aplicada

Prof. Dr. Vilmar Trevisan
Orientador

Profa. Dra. Virgínia M. Rodrigues
Co-orientadora

Porto Alegre, Julho de 2004.

CIP - CATALOGAÇÃO NA PUBLICAÇÃO

Hoppen, Carlos

Uma Generalização do Algoritmo de Gao para Fatoração de Polinômios / Carlos Hoppen.—Porto Alegre: PPGMAp da UFRGS, 2004.

118 p.: il.

Dissertação (mestrado) —Universidade Federal do Rio Grande do Sul, Programa de Pós-Graduação em Matemática Aplicada, Porto Alegre, 2004.
Orientador: Trevisan, Vilmar; Co-orientadora: Rodrigues, Virgínia M.

Dissertação: Matemática Aplicada
Computação Algébrica, Fatoração de Polinômios

Uma Generalização do Algoritmo de Gao para Fatoração de Polinômios

por

Carlos Hoppen

Dissertação submetida ao Programa de Pós-Graduação em Matemática Aplicada do Instituto de Matemática da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de

Mestre em Matemática Aplicada

Linha de Pesquisa: Algoritmos Algébricos e Numéricos

Orientador: Prof. Dr. Vilmar Trevisan

Co-orientadora: Profa. Dra. Virgínia M. Rodrigues

Banca examinadora:

Profa. Dra. Alicia Dickenstein
Universidad de Buenos Aires

Profa. Dra. Cydara Cavedon Ripoll
PPGMAT/IM/UFRGS

Prof. Dr. Paulo Ávila Zingano
PPGMAp/IM/UFRGS

Dissertação apresentada e aprovada em
26 de Julho de 2004.

Prof. Dr. Vilmar Trevisan
Coordenador

SUMÁRIO

LISTA DE ABREVIATURAS **5**

RESUMO **6**

ABSTRACT **7**

1 INTRODUÇÃO **8**

2 FATORANDO POLINÔMIOS EM DUAS VARIÁVEIS EM TEMPO POLINOMIAL **11**

2.1 Um algoritmo modular 11

2.2 O Levantamento de Hensel 19

2.3 Reticulados e Redução de Base 39

2.4 Um algoritmo em tempo polinomial para fatorar polinômios em duas variáveis 48

3 FATORANDO POLINÔMIOS VIA UMA EQUAÇÃO DIFERENCIAL **60**

3.1 Uma extensão do Algoritmo de Gao 60

3.2 As contribuições de Gao 84

3.3 Aplicações e Exemplos 96

4 CONCLUSÃO **104**

BIBLIOGRAFIA **106**

APÊNDICE A REDUÇÃO DA FATORAÇÃO EM VÁRIAS VARIÁVEIS A DUAS VARIÁVEIS **109**

APÊNDICE B DERIVAÇÕES **115**

LISTA DE ABREVIATURAS

$char(A)$	polinômio característico da matriz A
$cl_x(f)$	coeficiente líder do polinômio $f \in F[x, y]$ na variável x
col_iA	i-ésima coluna da matriz A
$cont_x(f)$	conteúdo do polinômio $f \in F[x, y]$ na variável x
$\bar{F}$	fecho algébrico do corpo F
$F(x)$	corpo de frações do anel $F[x]$
$I_{n\times n}$	matriz identidade de ordem n
$log\ n$	logaritmo na base dois de n
$M(n)$	tempo de multiplicação de dois polinômios univariados de grau n
mod, *módulo*	operação que associa um elemento a sua classe de resíduos
$O(f(n))$	ordem de complexidade
$pp_x(f)$	parte primitiva do polinômio $f \in F[x, y]$ na variável x
$Prob(\Omega)$	probabilidade de ocorrência do evento Ω
$quo(f, g)$	quociente da divisão euclideana de f por g
R/I	anel quociente (ou de classes de resíduos) do anel R pelo ideal $I \subseteq R$
$R[x_1, ..., x_n]$	anel de polinômios com coeficientes no anel R e indeterminadas $x_1, ..., x_n$
$Res_z(f(z), g(z))$	resultante dos polinômios f e g com respeito à variável z
$\|\cdot\| = \|\cdot\|_\infty$	norma do máximo de um vetor

RESUMO

A presente dissertação trata da fatoração de polinômios em duas variáveis sobre um corpo F. Mais precisamente, o trabalho traça o desenvolvimento histórico de uma estratégia modular que levou à resolução desse problema em tempo polinomial e culmina com a apresentação de um algoritmo publicado por S. Gao no ano de 2003, que determina simultaneamente as fatorações racional e absoluta de um dado polinômio. A nossa contribuição consiste na extensão desse algoritmo a casos que não satisfazem as condições prescritas pelo autor.

ABSTRACT

The present work deals with factorization of bivariate polynomials over a field F. More precisely, it follows the historical development of a modular strategy that has eventually led to the solution of this problem in polynomial time. In addition, we present an algorithm to find absolute and rational factorizations simultaneously, published by S. Gao in 2003. Our contribution lies in the extension of this algorithm to cases beyond the conditions prescribed by the author.

1 INTRODUÇÃO

A fatoração de polinômios é um problema antigo na história da Matemática. Isaac Newton já apresentou um algoritmo para esse problema em seu trabalho *Aritmetica Universalis*, publicado em 1707. Mas apenas no último século, em especial nas décadas a partir de 1970, a fatoração de polinômios foi retomada com ênfase na busca de métodos comprovadamente eficientes, bem como sua extensão a estruturas algébricas mais elaboradas. É importante observar o papel de destaque que o advento e o desenvolvimento de computadores tiveram na motivação desse estudo, pois, em um curto espaço de tempo, problemas outrora intratáveis começaram a ser confrontados e a ineficiência de muitos dos algoritmos intuitivos para sua resolução veio à tona.

Também se deve mencionar que o esforço para fatorar polinômios se tornou um dos grandes sucessos da Álgebra Computacional na década de 1980, quando foram apresentados algoritmos que solucionam esse problema em tempo polinomial sobre uma ampla classe de estruturas algébricas.

O tema dessa dissertação de mestrado é justamente a fatoração de polinômios, mais especificamente, a fatoração de polinômios em duas variáveis, e foi motivado por um problema particular: um algoritmo recentemente publicado recupera simultaneamente as fatorações racional e absoluta de um polinômio em duas variáveis a partir do espaço de soluções polinomiais de uma equação diferencial, cuja dimensão determina exatamente o número de fatores absolutamente irredutíveis do polinômio. Porém, apesar do sucesso teórico e prático, o seu funcionamento está restrito a polinômios sobre corpos de característica zero ou superior a uma determinada cota, que se relaciona com o momento em que o espaço de soluções começa a incluir soluções excedentes que impedem a recuperação da fatoração desejada. Mais do que isso: não é claro por que o espaço de soluções apresenta esse comportamento, visto que a cota na característica foi estabelecida de modo aparentemente artificial e o próprio autor do algoritmo menciona sua crença na existência de uma cota menor,

do que nossa intuição também se convence após alguns momentos de investigação. Essa multiplicidade de questões sem dúvida motivou que nos debruçássemos sobre tal problema, e o presente trabalho pretende justamente apresentar um compêndio de nossas investigações.

A primeira parte da dissertação, que compreende o segundo capítulo, é um apanhado histórico que procura retraçar o desenvolvimento de uma estratégia para fatorar polinômios em duas variáveis com complexidade polinomial em tempo. A escolha desse caminho reflete tanto seu caráter precursor, já que deu origem ao primeiro algoritmo em tempo polinomial para esse problema, quanto o seu caráter ilustrativo, pela diversidade de ferramentas fundamentais da Álgebra Computacional envolvidas, como, por exemplo, a computação por imagens homomórficas e a redução de base em reticulados.

O capítulo subseqüente engloba o corpo principal desse trabalho. A primeira seção generaliza o algoritmo para fatoração de polinômios em duas variáveis estabelecido por S. Gao, o que é a mais importante contribuição dessa dissertação. Dentre as questões levantadas na apresentação do problema, o nosso principal objetivo foi transpor as restrições decorrentes do surgimento de soluções excedentes no espaço vetorial de soluções polinomiais da equação diferencial, tanto no sentido de demonstrar que um de seus subespaços constitui o espaço adequado para o funcionamento do algoritmo, quanto no de o determinar efetivamente. Fomos capazes não somente de remover a restrição na característica do corpo para o qual existe um espaço vetorial com as propriedades desejadas, mas também de originar um algoritmo que determina esse espaço vetorial sobre corpos finitos. Para estabelecer tais resultados, utilizamos extensões das idéias originais de Gao.

A segunda seção desse capítulo se dedica à apresentação de resultados adicionais de Gao que levam à introdução do algoritmo desenvolvido por ele como caso particular da teoria apresentada na primeira seção. Exemplos e comentários sobre o comportamento do algoritmo percebidos durante o período de investigações serão incluídos em uma terceira seção, onde também haverá uma aplicação da teoria

que relaciona os fatores irredutíveis racionais de um polinômio a um segundo subespaço do espaço solução mencionado, o que nos fornece um teste de irredutibilidade de polinômios a duas variáveis.

Dois apêndices constam na dissertação, tratando de redução da fatoração em várias variáveis ao caso bivariado e da extensão de derivações. O primeiro destaca a importância do caso bivariado na fatoração de polinômios, pois mostra como a fatoração de polinômios em múltiplas variáveis pode ser reduzida ao caso bivariado, que não pode ser reduzido ao caso univariado por argumentos análogos. Crucial para essa redução é uma versão efetiva do teorema de irredutibilidade de Hilbert aqui apresentada. Também foram incluídas observações sobre como podemos tratar polinômios em várias variáveis do ponto de vista de estrutura de dados. O segundo apêndice procura sanar eventuais dúvidas de leitores na extensão de derivações, um conceito utilizado em algumas das demonstrações.

2 FATORANDO POLINÔMIOS EM DUAS VARIÁVEIS EM TEMPO POLINOMIAL

Esse capítulo é consagrado à apresentação de um algoritmo modular para a fatoração de polinômios em duas variáveis sobre um corpo F, supondo que se sabe fatorar polinômios em uma variável sobre F. Ele está organizado de tal forma que algumas das técnicas clássicas da Álgebra Computacional são introduzidas seguindo o fio histórico do seu desenvolvimento, na esperança de que essa estratégia auxilie na clareza do que é exposto, bem como na compreensão dos resultados que motivaram essa teoria. Além disso, há alusões recorrentes à fatoração de polinômios sobre $\mathbb{Z}[x]$, o anel de polinômios com coeficientes inteiros, devido à semelhança das idéias empregadas.

2.1 Um algoritmo modular

Seja então $f \in F[x, y]$. Suporemos que f é livre de quadrados, o que é de praxe no desenvolvimento de algoritmos para fatoração de polinômios. A redução do caso geral ao caso livre de quadrados é discutida em livros como o de D. Knuth [Knuth, 1969] e J. von zur Gathen e T. Gerhard [von zur Gathen e Gerhard, 1999]. Se a característica do corpo é zero, isso se faz por simples cálculos de máximo divisor comum. Para característica p, recaímos em corpos que não são perfeitos e que por isso exigem manipulações algébricas adicionais.

Em um primeiro momento, suporemos também que sabemos fatorar polinômios em uma variável sobre extensões algébricas de F, como no caso em que F é um corpo finito. No caso em que $F = \mathbb{Q}$, também se sabe fatorar polinômios em extensões algébricas finitas em tempo polinomial, apesar de a eficiência ser menor. Esse assunto não será tratado com mais profundidade no presente trabalho, e para maiores informações, recomendamos o trabalho precursor de S. Landau [Landau, 1985].

Portanto, será possível utilizar o fato de que, se $p \in F[y]$ é um polinômio irredutível, $F[y]/(p)$ é uma extensão algébrica de F. Em virtude disso, poderíamos pensar que, havendo meios de encontrar um polinômio irredutível em uma variável sobre F satisfazendo certas condições, o problema de fatoração em $F[x, y]$ seria reduzido ao problema fatorá-lo em $(F[y]/(p))[x]$, com posterior recuperação dos verdadeiros fatores em $F[x, y]$.

Note que um algoritmo seguindo as idéias acima é um algoritmo baseado na técnica de imagens homomórficas (também dito algoritmo modular), pois reduz o problema, originalmente em um anel A, a um problema em um anel quociente A/I, para certo ideal I de A. Intuitivamente, podemos considerar que se aplicou o homomorfismo canônico ao problema que tínhamos. Para que isso propicie alguma vantagem, é óbvio que devemos dispor de um método para a resolução desse novo problema e, nesse caso, resolveremos o problema original se suas soluções forem recuperáveis a partir das soluções do problema modular.

Para o nosso objetivo particular, a idéia básica será escolher um polinômio mônico irredutível em uma variável $p(y)$ de grau suficientemente grande para que os fatores originais possam ser recuperados da fatoração em $(F[y]/(p))[x]$. Mas conhecemos um modo simples de garantir isto: simplesmente tomaremos um polinômio p com grau superior a $2grau_y(f)$, pois é claro que todos os fatores de f, e mesmo os produtos entre dois fatores de f, têm grau em y inferior a esse número. Mais complicado do que isso será recompor os verdadeiros fatores de f em $F[x, y]$, pois polinômios irredutíveis sobre $F[x, y]$ não são em geral irredutíveis em $(F[y]/(p))[x]$. Por enquanto, essa recomposição será feita por tentativas.

Essa curta discussão motiva o seguinte algoritmo, onde os símbolos $cl_x(f)$ e $pp_x(f)$ denotam o coeficiente líder e a parte primitiva do polinômio f com respeito à variável x, respectivamente:

Algoritmo 2.1.1. *Fatoração de polinômios em $F[x,y]$ via primo grande*

Entrada: *Um polinômio livre de quadrados $f \in F[x,y]$,*
com $(grau_x f, grau_y f) = (m,n)$.

Saída: *O conjunto de fatores irredutíveis $\{f_1,...,f_s\}$ de f em $F[x,y]$.*

1. *se $n = 1$, então devolva $\{f\}$.*
   $b \leftarrow cl_x(f), \quad l \leftarrow n + grau\ b + 1$
2. *encontre p irredutível em $F[y]$ com grau B igual ou superior a l.*
3. $\{$*Fatoração Modular*$\}$
   determine $g_1,...,g_r \in F[x,y]$ mônicos e irredutíveis sobre $F[y]/(p)$,
   com grau em y inferior a B tais que $f \equiv bg_1...g_r \ mod\ p$.
5. $\{$*Inicialização do conjunto de índices T de fatores modulares ainda não*
   considerados, do conjunto G de fatores encontrados, e do polinômio $f^\star$ a ser fatorado$\}$
   $T \leftarrow \{1,2,...,r\}, \ \ s \leftarrow 1, \ \ G \leftarrow \emptyset, \ \ f^\star \leftarrow f$
6. $\{$*Combinação de fatores*$\}$
   enquanto $2s \leq \sharp T$ faça
7. *para todos subconjuntos $S \subseteq T$ de cardinalidade $\sharp S = s$ faça*
8. *calcule $g^\star$, $h^\star \in F[x,y]$ com grau em y inferior a B satisfazendo*
   $g^\star \equiv b\prod_{i\in S} g_i \ mod\ p$ e $h^\star \equiv b\prod_{i\in T\setminus S} g_i \ mod\ p$
9. *se $grau_y(g^\star h^\star) = grau_y(bf^\star)$ então*
   $T \leftarrow T\setminus S$, $G \leftarrow G \cup pp_x(g^\star)$,
   $f^\star \leftarrow pp_x(h^\star), b \leftarrow cl_x(f^\star)$
   interrompa o laço 7 e vá a 6.
10. $s \leftarrow s + 1$
11. *devolva $G \cup \{f^\star\}$*

Antes de demonstrarmos a validade desse algoritmo, faremos algumas observações e apresentaremos um exemplo que ilustra sua aplicação.

Observações

1. O passo 4 do algoritmo foi omitido intencionalmente para garantir a compatibilidade com algoritmos que virão a seguir.

2. A nomenclatura "por primo grande" é motivada pelo algoritmo análogo para polinômios f em $\mathbb{Z}[x]$, que calcula a fatoração de f sobre $\mathbb{Z}_p$, onde p é um número primo grande (determinado pela cota de Mignotte), de tal forma que os fatores sobre $\mathbb{Z}$ possam ser recuperados. No nosso caso, o primo é o polinômio irredutível $p(y)$, que de fato é um elemento primo do domínio de integridade $F[y]$, e a cota é simplesmente o grau do polinômio.

Contraposto a esse algoritmo, teríamos a fatoração por primos pequenos, que utiliza diversos primos menores. Individualmente, eles não garantem a recuperação imediata da solução desejada, que será obtida da combinação das soluções dos diversos problemas pequenos. Porém, essa estratégia, bem sucedida em uma ampla gama de problemas da Álgebra Computacional, não se adeqúa a nosso problema, pois o fato mais problemático de nosso algoritmo é justamente a recombinação dos diferentes fatores irredutíveis módulo p que correspondem a um mesmo fator irredutível sobre o anel original, que deriva do fato de que $F[y]/(p_1p_2...p_m)$, para polinômios irredutíveis distintos $p_1, p_2, ..., p_m$ na variável y não é um domínio de fatoração única para $m \geq 2$.

Exemplo 2.1.2. *Seja o polinômio*

$$f(x,y) = x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1$$

em $F_2[x,y]$ *(em nossa notação,* $F_2 = \mathbb{Z}_2 = GF(2)$*). Vamos utilizar o algoritmo anterior para encontrar sua fatoração. Utilizando um algoritmo para determinar o máximo divisor comum, verificamos que* f *é livre de quadrados, pois temos que* $mdc(f, \frac{\partial f}{\partial x}) = mdc(f, \frac{\partial f}{\partial y}) = 1$.

Aplicamos então nosso algoritmo para polinômios livres de quadrados. Esse algoritmo considera esse polinômio em $(F_2[y])[x]$*, isto é, na forma*

$$f(x,y) = y^4x^5 + (y^5 + y^4)x^4 + yx^2 + (y^2 + y + 1)x + y + 1.$$

Nesse momento, devemos escolher um "primo grande" para efetuar a fatoração: o grau em y de f é igual a 5, e $b = y^4$. Escolheremos então o polinômio irredutível $p(y) = y^{10} + y^3 + 1$ em $F_2[y]$ (grau $p = 10 \geq 10 = grau_y(f) + grau\ b + 1$) e consideraremos $f = f(x)$ em $(F_2[y]/(p))[x] \simeq F_{2^{10}}[x]$. Sabemos como obter a fatoração de polinômios em uma variável sobre esse último corpo finito. Fazendo as contas, segue que $g_1 = x^2 + (y^9 + y^2)x + y^8 + y^5 + y^4 + y^3 + 1$, $g_2 = x^2 + (y^9 + y^2)x + y^5 + y^4 + y^3 + y + 1$ e $g_3 = x + y + 1$ são os polinômios irredutíveis que satisfazem $f \equiv bg_1g_2g_3$ em $(F_2[y]/(p))[x]$, onde $b = cl_x(f) = y^4$.

Dirigimo-nos agora ao passo 5, em que devemos recombinar os fatores g_1, g_2, g_3 para obter os fatores irredutíveis de f em $F[x, y]$. Inicializam-se

$$T \leftarrow \{1, 2, 3\},\ s \leftarrow 1,\ G \leftarrow \emptyset,\ f^\star \leftarrow f$$

Como $2 = 2s \leq \sharp T = 3$, analisaremos os subconjuntos S de T de cardinalidade um. Tomemos $S_1 = \{1\}$: calculam-se $g^\star = y^4x^2 + y^3x + y^9 + y^8 + y^7 + y^5 + y^4 + y^2$ e $h^\star = y^4x^3 + (y^5 + y^4 + y^3)x^2 + (y^9 + y^8 + y^7 + y^5 + y^3)x + y^7 + y^6 + y^4 + y^3 + 1$. Vemos que $grau_y(g^\star h^\star) = 18 > 9 = grau_y(bf^\star)$, logo S_1 não dá origem a um fator irredutível de f em $F[x, y]$. Seja então $S_2 = \{2\}$. Nesse caso, $g^\star = y^4x^2 + y^3x + y^9 + y^8 + y^7 + y^5 + y^4$ e $h^\star = y^4x^3 + (y^5 + y^4 + y^3)x^2 + (y^9 + y^8 + y^7 + y^5 + y^3 + y^2)x + y^7 + y^6 + y^4 + y^2 + 1$, repetindo $grau_y(g^\star h^\star) = 18 > 9 = grau_y(bf^\star)$. Em uma terceira tentativa, temos $S_3 = \{3\}$. Calculamos $g^\star = y^4x + y^5 + y^4$ e $h^\star = y^4x^4 + yx + 1$. Agora, verifica-se que $grau_y(g^\star h^\star) = 9 = grau_y(bf^\star)$, ou seja, a condição do passo 9 é satisfeita, Portanto,

$$T \leftarrow T \backslash S = \{1, 2\},\ G \leftarrow G \cup pp_x(g^\star) = \{x + y + 1\},$$
$$f^\star \leftarrow pp_x(h^\star) = y^4x^4 + yx + 1,\ b \leftarrow cl_x(f^\star) = y^4$$

O passo 7 é interrompido e voltamos ao passo 6, onde temos agora $2 = 2s \leq 2 = \sharp T = 2$. Mas todos os subconjuntos de cardinalidade um de T já foram analisados. Logo, chegamos ao passo 10 e $s \leftarrow 2$. A condição do passo 6 não é mais satisfeita, de forma que alcançamos o passo 11 e devolvemos

$$G \cup \{f^\star\} = \{x + y + 1, x^4y^4 + xy + 1\}.$$

Obtivemos a fatoração irredutível

$$f(x,y) = x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1 = (x+y+1)(x^4y^4 + xy + 1)$$

em $F_2[x,y]$.

A seguir, vamos demonstrar a validade desse algoritmo e analisar sua complexidade em tempo. Na análise de complexidade, utilizaremos duas notações bastante comuns. A primeira delas se refere à ordem O de complexidade e, quando dizemos que $g(n) \in O(f(n))$, ou, por abuso de nomenclatura, que g é de $O(f(n))$, queremos dizer que existem $c, N \in \mathbb{N}$ tais que $f(n) \leq cg(n)$ para todo $n \geq N$. Isto é, a ordem de complexidade é uma majoração de f a menos de constantes. A segunda notação que introduziremos diz respeito à multiplicação de dois polinômios em uma variável de grau limitado por n sobre um corpo F. Para não nos preocuparmos com propriedades particulares do corpo ou com o algoritmo utilizado, estabeleceremos que o custo envolvido será $M(n)$ operações.

Teorema 2.1.3. *O algoritmo (2.1.1) funciona. O custo esperado para o passo* 3 *é de* $O(mnM(m)log(qm))$*, se* F *é um corpo finito de* q *elementos, enquanto que os passos* 8 *e* 9 *exigem* $O(M(n)(mlog(n) + mM(m)))$*, havendo, no máximo,* 2^{m+1} *iterações.*

Demonstração

Inicialmente, observemos que a condição do passo 9 vale se, e somente se, $g^\star h^\star = bf^\star$. A necessidade é trivial. Vejamos a suficiência: sejam $g^\star \equiv b\prod_{i\in S} g_i \ mod\ p$ e $h^\star \equiv b\prod_{i\in T\setminus S} g_i \ mod\ p$. Logo, $g^\star h^\star \equiv bf^\star \ mod\ p$. Note que $grau_y(bf) \leq grau_y b + grau_y f < l \leq grau_y p$. Mas ambos os lados da congruência são polinômios de mesmo grau em y, e portanto são iguais.

Dado um fator $u \in F[x,y]$ de f, denotemos por $\mu(u)$ o número de fatores mônicos irredutíveis que dividem u módulo p. Da unicidade da fatoração, esses fatores formam um subconjunto de $\{g_1, ..., g_r\}$.

Afirmação: A cada passagem pelo passo 6, os seguintes invariantes são verificados:

(i) $f^\star \equiv b \prod_{i \in T} g_i \ mod \ p$

(ii) $b = cl_x(f^\star)$

(iii) $f = f^\star \prod_{g \in G} g$

(iv) Cada polinômio em G é irredutível

(v) Para cada fator irredutível u de $f^\star$, $\mu(u) \geq s$

A demonstração dessa afirmação será feita por indução.

Os invariantes são triviais na primeira passagem por 6. Suponha que eles sejam válidos antes do passo 8. Se, para todos os subconjuntos S de T de cardinalidade s, a condição 9 for rejeitada, então $f^\star$ e G não se alteram, assim como as quatro primeiras invariâncias.

Para mostrar que a última também permanece válida, basta provar que $f^\star$ não possui fator g com $\mu(g) = s$. Suponha, por absurdo, que existe g nessas condições. Logo, $f^\star = gh$, para certo $h \in F[x, y]$. Então, há $S \subseteq T$ de cardinalidade s tal que $g \equiv cl_x(g) \prod_{i \in S} g_i \ mod \ p$. É claro também que $cl_x(g)cl_x(h) = cl_x(f^\star) = b$, $cl_x(h)g \equiv b \prod_{i \in S} g_i \equiv g^\star \ mod \ p$ e $cl_x(g)h \equiv b \prod_{i \in T \setminus S} g_i \equiv h^\star \ mod \ p$. Como o grau de cada um dos polinômios em y é inferior ao de p, as equivalências acima são igualdades. Conseqüentemente, $g^\star h^\star = bf^\star$ e a condição 9 é válida para S ?!!

Agora, seja S um subconjunto de s elementos de T que satisfaz a condição 9. Denotaremos as atualizações de $T, G, b, f^\star$ por $T', G', b', f^{\star\prime}$. Observemos também que, como $f^\star$ é primitivo, $pp_x(g^\star)pp_x(h^\star) = pp_x(g^\star h^\star) = pp_x(bf^\star) = f^\star$. Nesse caso:

(i) $f^{\star\prime} = pp_x(h^\star) \equiv cl_x(h^\star) \prod_{i \in T \setminus S} g_i = b' \prod_{i \in T'} g_i \ mod \ p.$

(ii) $b' = cl_x(pp_x(h^\star)) = cl_x(f^{\star\prime})$

(iii) Pela hipótese de indução, $f = f^\star \prod_{g \in G} g = pp_x(h^\star)pp_x(g^\star) \prod_{g \in G} g = f^{\star\prime} \prod_{g \in G'} g$

(iv) Suponha, por absurdo, que $g^\star$ é redutível. Logo, um fator próprio de $g^\star$ teria fatoração formada por um subconjunto próprio S' de elementos de S. Mas, nesse caso, $\sharp S' < \sharp S$, de forma que S' teria sido escolhido no momento em que $s = \sharp S'$ e teria sido retirado de S.

(v) Nada se altera quanto a esse item, logo ele decorre diretamente da hipótese de indução.

Isso conclui a demonstração da afirmação. Resta apenas demonstrar que, se $2s > \sharp T$, então $f^\star$ é um elemento irredutível em $F[x, y]$. Sejam $g \in F[x, y]$ um fator irredutível de $f^\star$ e $h = \frac{f^\star}{g}$. Pela última das invariâncias, $\mu(g) \geq s$ e, como $\mu(g)+\mu(h) = \sharp T$, $\mu(h) \leq \sharp T - s < \frac{\sharp T}{2}$. Portanto, h é uma constante, o que estabelece a demonstração.

Vejamos a complexidade desse algoritmo. Os passos 1 e 2 não têm custo elevado. O passo 3, no caso em que $F = F_q$ é um corpo finito, exige $O(mM(m)log(\bar{q}m))$, pois fatora um polinômio de grau m (na variável x) sobre um corpo finito com $\bar{q}$ elementos. Mas, como a fatoração é feita em $(F[y]/(p))[x]$ e $grau_y(p)$ é da ordem de $l \leq 2n + 1$, temos que $\bar{q}$ é da ordem de q^{2n}. Segue que o passo 3 é limitado por $O(mnM(m)log(qm))$ operações aritméticas sobre F_q.

O custo de se computar $g^\star$ e $h^\star$ no passo 8 é de $O(M(m)log\ m)$ adições e multiplicações de polinômios em $F[y]$ de grau limitado por n, o que nos dá $O(M(m)log\ mM(n))$ operações em F. Para calcular as partes primitivas dos polinômios no passo 9, são exigidas $O(mM(n)log\ n)$ operações. O número de iterações dos passos 8 e 9 é obtido da seguinte forma: entre duas ocasiões em que a condição no passo 9 é verdadeira, existem no máximo $2^{\sharp T}$ execuções dos passos 8 e 9. Mas $\sharp T$ se reduz em pelo menos uma unidade se a condição é verdadeira, logo o número de iterações é limitado por $\sum_{i=1}^{r} 2^i \leq 2^{r+1} \leq 2^{m+1}$. $\square$

O algoritmo acima resolve o problema da fatoração de polinômios em $F[x, y]$ quando sabemos fatorar sobre extensões algébricas de F, mas apresenta dois problemas graves. O primeiro está no fato de que ele não é aplicável com

eficiência a polinômios em duas variáveis sobre $\mathbb{Q}[x, y]$, que formam uma classe importantíssima de polinômios. O segundo consiste no fato de o algoritmo ser exponencial no pior caso, resultado de nossa incapacidade em arranjar os fatores modulares para recuperar os fatores procurados de forma eficaz. Apesar de termos apresentado uma cota pessimista no número de iterações, existem de fato casos em que cotas muito ruins vigoram, como para classes de polinômios ciclotômicos e de Swinnerton-Dyer, que são discutidas no trabalho de E. Kaltofen, D.R. Musser e B.D. Saunders [Kaltofen et al., 1983] para polinômios em uma variável em $\mathbb{Z}[x]$. Na seqüência desse trabalho, procuraremos transpor essas dificuldades.

2.2 O Levantamento de Hensel

Em 1918, Kurt Hensel [Hensel, 1918] desenvolveu um método para calcular a fatoração de polinômios módulo p^l, onde p é um número primo e l um inteiro positivo, a partir de sua fatoração módulo p. Embora Hensel tenha se concentrado nos números inteiros, a idéia pode ser aproveitada para a fatoração de polinômios em duas variáveis, pois depende de propriedades algébricas gerais.

Por questões de clareza e motivação, partiremos de uma idéia simples e adicionaremos os detalhes necessários. Sejam R um anel (comutativo, com unidade), $f, g, h \in R[x]$ e $m \in R$ tais que $f \equiv gh \ mod \ m$. Desejamos "erguer" essa fatoração para $f \equiv \hat{g}\hat{h} \ mod \ m^2$, ou seja, aproveitar a fatoração conhecida módulo m para obter a fatoração módulo m^l. Vamos supor que conhecemos $s, t \in R[x]$ com a propriedade de que $sg + th \equiv 1 \ mod \ m$ (em particular, g e h são relativamente primos módulo m). Quando $R/(m)$ é um corpo, podemos obter s e t facilmente pelo Algoritmo de Euclides Estendido.

Agora, calculamos $e = f - gh$, $\hat{g} = g + te$ e $\hat{h} = h + se$. Logo, $f - \hat{g}\hat{h} = e(1 - gs - ht) - ste^2$, e, como estamos supondo $e \equiv 0 \ mod \ m$ e $1 - gs - ht \equiv 0 \ mod \ m$, vem que $f - \hat{g}\hat{h} \equiv 0 \ mod \ m^2$.

Se estivermos em um domínio e partirmos de m igual a um elemento primo p, procedendo indutivamente (e simultaneamente erguendo a congruência $sg + th \equiv 1$) podemos erguer a fatoração módulo potências arbitrárias de p.

Exemplo 2.2.1. *Voltemos a nosso exemplo, em que tínhamos o polinômio livre de quadrados* $f(x, y) = x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1$ *em* $F_2[x, y]$. *Consideremos o corpo* $K = F_2[y]/(p)$, *onde* $p = y^4 + y^3 + y^2 + y + 1$, *e vejamos* f *como polinômio em* $K[x]$. *Verifica-se que*

$$f = ((y^3 + y^2 + y + 1)x^3 + (y^3 + y^2 + y)x^2 + (y^3 + y^2 + 1)x + y^3 + y)(x^2 + y^2 + 1)$$

em $K[x]$. *Vamos utilizar a sugestão acima para obter uma fatoração de* f *módulo* p^2. *Para tanto, calculamos* $e = f - gh = (y^4+y^3+y^2+y+1)x^5+(y^5+y^4+y^3+y^2+y)x^4+(y^5+y^4+y^3+y^2+y)x^3+(y^5+y^4+y^3+y^2+y)x^2+(y^5+y^4+y^3+y^2+y)x+y^5+1$, $\hat{g} = g+te = (y^7+y^6+y^5+y^4+y^3)x^6+(y^8+y^7+y^5+y^3+y^2+1)x^5+(y^8+y^6+y^3+y)x^4+(y^8+y^6+y^2+1)x^3+(y^8+y^6+y^2)x^2+(y^8+y^7+y^5+y^4+y^3+y^2+y+1)x+y^7+y^6+y^5+y^3+y^2+1$ *e* $\hat{h} = h + se = (y^7 + y^5 + y^2 + 1)x^5 + (y^8 + y^6 + y^3 + y)x^4 + (y^8 + y^6 + y^3 + y)x^3 + (y^8 + y^6 + y^3 + y + 1)x^2 + (y^8 + y^6 + y^3 + y)x + y^8 + y^7 + y^6 + y^5 + y^3 + y$. *Fazendo as contas, verificamos que* $f - \hat{g}\hat{h} \equiv 0 \ mod \ p^2$.

Obtemos então a fatoração $f = ((y^7 + y^5 + y^2 + 1)x^5 + (y^4 + y^3 + y^2 + y+1)x^4+(y^4+y^3+y^2+y+1)x^3+(y^4+y^3+y^2+y)x^2+(y^4+y^3+y^2+y+1)x+y^7+y^5+y^4+y^3+y^2+y+1)((y^7+y^6+y^5+y^4+y^3)x^6+(y^7+y^6+y^5+y^4+y^3)x^5+(y^4+y^3+y^2+y+1)x^4+y^4x^3(y^4+1)x^2+(y^7+y^6+y^5+y^3+y)x+y^7+y^6+y^5+y^3+y^2+1)$ *no anel* $F[y]/(p^2)[x]$.

Esse exemplo já mostra uma desvantagem desse método: os graus de $\hat{g}$ e $\hat{h}$ são maiores do que os de g e h e, em particular, a soma de seus graus excede o grau de f. Para superar esse empecilho, que acarreta o que se denomina crescimento das expressões intermediárias, recorreremos à divisão com resto em $R[x]$. Como R

não é necessariamente corpo, essa divisão não está em geral definida. Se efetuarmos a divisão apenas por polinômios mônicos, contudo, não há problemas de definição.

O resultado disso está no seguinte algoritmo, que ergue uma fatoração de f em dois fatores módulo m a uma fatoração de dois fatores módulo m^2, também conhecido como levantamento quadrático de Hensel:

Algoritmo 2.2.2. *Passo de Hensel*

Entrada: *Um elemento m pertencente ao anel comutativo R, e polinômios $f, g, h, t, s \in R[x]$ tais que $f \equiv gh$ e $sg + th \equiv 1 \ mod \ m$, h é mônico,*
$grau(f) = n = grau(g) + grau(h)$, $grau(s) < grau(h)$, $grau(t) < grau(g)$.

Saída: *Polinômios $g^\star, h^\star, s^\star, t^\star \in R[x]$ tais que $f \equiv g^\star h^\star$*
e $s^\star g^\star + t^\star h^\star \equiv 1 \ mod \ m^2$, $h^\star$ é mônico, $g^\star \equiv g$, $h^\star \equiv h$, $s^\star \equiv s$, $t^\star \equiv t \ mod \ m$,
$grau(g^\star) = grau(g)$, $grau(h^\star) = grau(h)$, $grau(s^\star) < grau(h^\star)$, $grau(t^\star) < grau(g^\star)$

1. *calcule $e, q, r, g^\star, h^\star \in R[x]$ tais que*
   $grau(r) < grau(h)$, $e \equiv f - gh$, $es \equiv qh + r$, $g^\star \equiv g + te + qg$ e $h^\star \equiv h + r \ mod \ m^2$.
2. *calcule $b, c, d, s^\star, t^\star \in R[x]$ tais que*
   $grau(d) < grau(h^\star)$, $b \equiv sg^\star + th^\star - 1$, $sb \equiv ch^\star + d$, $s^\star \equiv s - d$ e $t^\star \equiv t - tb - cg^\star \ mod \ m^2$.
3. *devolva $g^\star, h^\star, s^\star, t^\star$*

Para ilustrar o funcionamento do algoritmo, vejamos como ele se aplica ao exemplo anterior:

Exemplo 2.2.3. *Lembremos que se dispunha da fatoração*

$$f = gh = ((y^3 + y^2 + y + 1)x^3 + (y^3 + y^2 + y)x^2 + (y^3 + y^2 + 1)x + y^3 + y)(x^2 + y^2 + 1)$$

em $(F_2/(p))[x]$, que queríamos estender a uma fatoração módulo p^2, dado que os elementos $s = y^3 + y^2 + y + 1$ e $t = y^3x + y^2 + y + 1$ satisfazem $sg + th \equiv 1 \ mod \ p$.

Pelo algoritmo do Passo de Hensel (observe que todas as condições de entrada do algoritmo são satisfeitas), vem que $e = (y^4 + y^3 + y^2 + y + 1)x^5 + (y^5 +$

$y^4+y^3+y^2+y)x^4+(y^5+y^4+y^3+y^2+y)x^3+(y^5+y^4+y^3+y^2+y)x^2+(y^5+y^4+y^3+y^2+y)x+y^5+1$. *Pela divisão euclideana, obtêm-se* $q=(y^7+y^5+y^2+1)x^3+(y^4+y^3+y^2+y+1)x^2+(y^7+y^2)x+y^6+y^5+y^4+y^3+y^2$ *e* $r=(y^5+1)x+y^6+y^5+y+1$ *e, desses valores, segue que* $g^\star=y^4x^3+(y^7+y^3+y)x^2+(y^6+y^4)x+y^3+y$ *e* $h^\star=x^2+(y^5+1)x+y^6+y^5+y^2+y$. *Fazendo as contas, verifica-se que* $f-g^\star h^\star\equiv 0 \ mod\ p^2$. *Note que agora obtivemos* $g^\star$ *e* $h^\star$ *com graus em* x *iguais a* 3 *e* 2, *respectivamente, contra graus* 6 *e* 5 *obtidos para* $\hat{g}$ *e* $\hat{h}$ *pelo método anterior.*

O passo 2 *do algoritmo se destina a erguer os polinômios* s *e* t *a* $s^\star$ *e* $t^\star$ *satisfazendo* $s^\star g^\star+t^\star h^\star\equiv 1 \ mod\ p^2$, *o que garante a possibilidade de utilização iterada do passo de Hensel. Fazendo as contas, chega-se a* $b=(y^7+y^6+y^5+y^4+y^3)x^3+(y^6+y)x^2+(y^7+y^6+y^5+1+y^2+y)x$, $c=(y^6+y^5+y^4+y^3+y^2)x+y^5+1$ *e* $d=y^7+y^5+y^2+1$. *Portanto,* $s^\star=y^7+y^5+y^3+y$ *e* $t^\star=y^3x+y^4+y^3$.

O próximo teorema estabelecerá a validade do algoritmo e analisará sua complexidade.

Teorema 2.2.4. *O algoritmo funciona. Se as entradas do algoritmo têm grau em* y *limitado pela cota* $D>0$, *ele utiliza* $O(M(n)M(D))$ *operações no corpo* F.

Para provar esse resultado, utilizaremos o seguinte lema técnico:

Lema 2.2.5. *Sejam* R *um anel e* $f,g\in R[x]$, *com* g *não-nulo e mônico. Então,*

(i) *Existem polinômios* q *e* r *univocamente determinados, tais que* $f=qg+r$ *e grau* $r<$ *grau* g *ou* $r=0$.

(ii) *Se* $f\equiv 0 \ mod\ m$ *para algum* m *em* R, *então* $q\equiv r\equiv 0 \ mod\ m$.

Demonstração

O item (i) é um resultado bem conhecido em anéis de polinômios. Demonstremos o item (ii): seja $m\in R$ tal que $f\equiv 0 \ mod\ m$. Portanto, existe h em $R[x]$ tal que $f=mh$. Mas, aplicando o item (i) a h, obtemos q_1,r_1 em $R[x]$,

com $grau\ r_1 < grau\ g$ ou $r_1 = 0$, tais que $h = q_1 g + r_1$. Logo, $f = mh = mq_1 g + mr_1$. Como $m \in R$, é claro que $grau\ mr_1 \leq grau\ r_1$, logo $\hat{q} = mq_1$ e $\hat{r} = mr_1$ satisfazem as condições do item (i). Pela unicidade, temos $q = \hat{q}$, $r = \hat{r}$, e, conseqüentemente, $q \equiv r \equiv 0\ mod\ m$, o que conclui a demonstração do lema.

Demonstração do teorema

Inicialmente, vejamos que o algoritmo (2.2.2) funciona. Observe, que, por definição, $f - g^\star h^\star \equiv f - (g + te + qg)(h + es - qh)\ mod\ m^2$, ou, reagrupando os termos da expressão à direita, $f - g^\star h^\star \equiv f - gh - (sg + th)e - ste^2 - (sg - th)qe + ghq^2\ mod\ m^2$. Mas, da definição de e, essa última expressão é equivalente a $(1 - sg - th)e - ste^2 - (sg - th)qe + ghq^2\ mod\ m^2$. Por hipótese, sabemos que $1 - sg - th \equiv 0 \equiv e\ mod\ m$. Portanto, $0 \equiv es \equiv qh + r\ mod\ m$. Aplicando o lema, obtemos $q \equiv r \equiv 0\ mod\ m$, e todas essas equivalências módulo m implicam $(1 - sg - th)e \equiv e^2 \equiv qe \equiv q^2 \equiv 0\ mod\ m^2$. Portanto, $f - g^\star h^\star \equiv (1 - sg - th)e - ste^2 - (sg - th)qe + ghq^2 \equiv 0\ mod\ m^2$.

Além disso, como $h^\star \equiv h + r\ mod\ m^2$, vale que $h^\star \equiv h + r \equiv h\ mod\ m$. Analogamente, $g^\star \equiv g + te + qg \equiv g\ mod\ m$. Do fato de que $grau\ r < grau\ h$, segue $h^\star$ tem o mesmo grau de h e é mônico, o que, por sua vez, acarreta $grau\ g^\star = grau\ f - grau\ h^\star = grau\ f - grau\ h = grau\ g$. Argumentos muito similares são empregados para demonstrar as propriedades análogas de $s^\star$ e $t^\star$.

A análise desse algoritmo é bastante simples: notamos que polinômios $f(x, y)$ podem ser escritos na forma $(f(y))(x)$, de forma que toda operação aritmética em $F[x, y]$ (adição, multiplicação, divisão com resto) exige $O(M(n)M(D))$ operações em F se feita entre polinômios com graus em x e y limitados por n e D, respectivamente. Mas o número de operações em $F[x, y]$ é constante em nosso algoritmo, logo a sua complexidade é de fato $O(M(n)M(D))$ operações. □

Corolário 2.2.6. *Dado um inteiro positivo l e supondo a especificação do algoritmo, podemos calcular polinômios satisfazendo as condições de saída do algoritmo anterior com m^2 substituído por m^l.*

Demonstração

Se o Passo de Hensel for aplicado indutivamente, obtêm-se elementos módulo $m^2, m^{2^2}, m^{2^3}, ...$ satisfazendo as condições de saída do algoritmo (2.2.2) com m^2 substituído por m^{2^l} para l adequado. Basta então observar que uma fatoração módulo m^{l_1} nas condições prescritas origina uma fatoração módulo m^{l_2} nessas mesmas condições se $l_1 > l_2$, isto é, é suficiente fazer o levantamento módulo m elevado a potências de 2. □

Agora, veremos que o procedimento acima, criado como que por inspeção, é essencialmente único.

Teorema 2.2.7. *Unicidade do Levantamento de Hensel*

Sejam R um anel comutativo com unidade, $m \in R$ um elemento que não divide zero, l um inteiro positivo e $g, h, g^\star, h^\star, s, t \in R[x]$ polinômios não nulos tais que:

- $sg + th \equiv 1 \ mod \ m$
- *os coeficientes líder de g e h não dividem zero em R módulo m*
- *g e $g^\star$, h e $h^\star$ têm mesmo grau e termo líder em $R[x]$ e coincidem módulo m.*

Se $gh \equiv g^\star h^\star \ mod \ m^l$, então $g \equiv g^\star \ mod \ m^l$ e $h \equiv h^\star \ mod \ m^l$.

Em outras palavras, dois levantamentos de fatores módulo m a fatores módulo m^l coincidem.

Demonstração

Suponhamos, por absurdo, que $g \neq g^\star \ mod \ m^l$ ou $h \neq h^\star \ mod \ m^l$. Seja $i \in \{1, 2, ..., l-1\}$ maximal tal que m^i divide $g - g^\star$ e $h - h^\star$. Então, $g^\star - g = um^i$, $h^\star - h = vm^i$ para certos u e v em R. Sem perda de generalidade, suponhamos que

m não divide u. Mas $0 \equiv g^\star h^\star - gh = g^\star(h^\star - h) + h(g^\star - g) = (g^\star v + hu)m^i \ mod \ m^l$.

Como m não divide zero em R, m divide m^{l-i} que, pela congruência acima, divide $g^\star v + hu$. Denotaremos por uma barra a redução módulo m. Das hipóteses e do que vimos até aqui, segue que $\bar{s}\bar{g} + \bar{t}\bar{h} = \bar{1}$, $\bar{g^\star} = \bar{g}$ e $\bar{g^\star}\bar{v} + \bar{h}\bar{u} = \bar{0}$. Assim, $\bar{0} = \bar{t}(\bar{g^\star}\bar{v} + \bar{h}\bar{u}) = \bar{t}\bar{g}\bar{v} + (\bar{1} - \bar{s}\bar{g})\bar{u} = (\bar{t}\bar{v} - \bar{s}\bar{u})\bar{g} + \bar{u}$. Mas essa última igualdade implica a divisibilidade de $\bar{u}$ por $\bar{g}$. Por outro lado, $lc(g) = lc(g^\star)$ e $grau(\bar{g}) = grau(g) = grau(g^\star)$, de forma que $grau(u) < grau(\bar{g})$, pois $g^\star - g = um^i$. Logo, $\bar{u} = 0$, contradizendo o fato de que m não divide u. □

O seguinte corolário será útil quando trabalharmos com redução de bases em reticulados:

Corolário 2.2.8. *Sejam R um domínio Euclideano, $p \in R$ primo, l um inteiro positivo e $f, g, u \in R[x]$ tais que p não divide $cl_x(f)$, $f \ mod \ p$ é livre de quadrados, g divide f em $R[x]$, e u é mônico, não constante, e divide tanto f módulo p^l quanto g módulo p. Então, u divide g módulo p^l.*

Demonstração

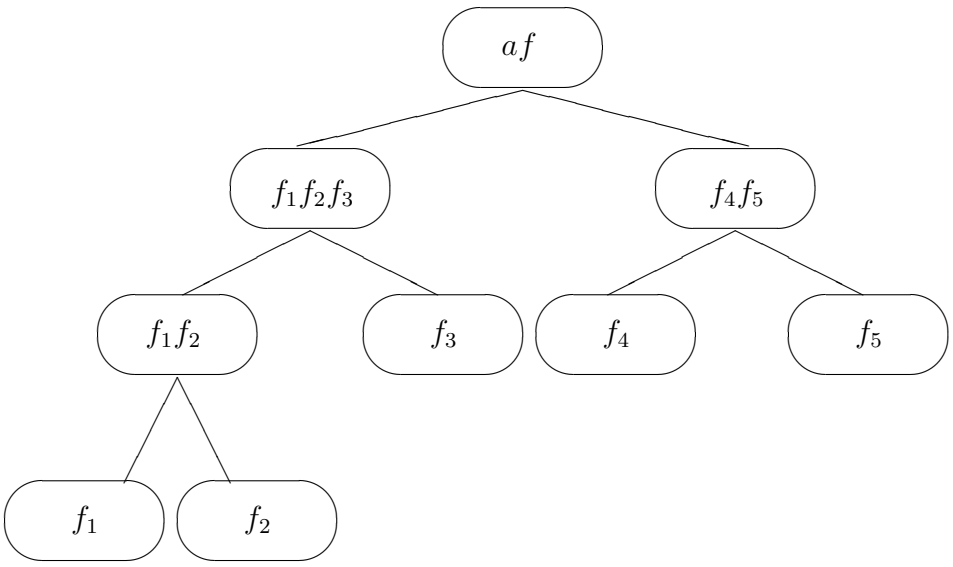
Sejam polinômios h, v, w em $R[x]$ tais que $f = gh \equiv uw \ mod \ p^l$ e $g = uv \ mod \ p$. Já que $f \ mod \ p$ é livre de quadrados, $g \ mod \ p$ também o será e $mdc(u \ mod \ p, v \ mod \ p) = 1$ em $F_p[x]$, onde $F_p = R/(p)$ é um corpo. Logo, é possível obter $s, t \in F_p[x]$, $grau \ s < grau \ v$, $grau \ t < grau \ u$, tais que $su + tv \equiv 1 \ mod \ p$. Aplicando o Passo de Hensel iterativamente, arranjamos polinômios $u^\star, v^\star$ satisfazendo $u^\star \equiv u$ e $v^\star \equiv v$ módulo p e $g \equiv u^\star v^\star$ módulo p^l. Mas $uvh \equiv gh \equiv uw \ mod \ p$ e, como $F_p[x]$ é um domínio de integridade, $vh \equiv w \ mod \ p$.

Portanto, $v^\star h \equiv vf \equiv w \ mod \ p$ e $u^\star(v^\star h) \equiv gh \equiv uw \ mod \ p^l$. Aplicamos o teorema anterior (lembre que g e h são relativamente primos e u e v são relativamente primos módulo p) e obtemos $u \equiv u^\star \ mod \ p^l$, e finalmente $g \equiv uv^\star$ módulo p^l. □

Há benefícios potenciais de se recorrer à fatoração de polinômios com dois fatores módulo um primo pequeno e depois erguê-la à fatoração módulo um elemento suficientemente grande. Se conseguirmos estender essa técnica a polinômios com múltiplos fatores a um custo razoável, esse método parece promissor, pois o levantamento de fatores é obtido apenas pela resolução de equações modulares e pela aplicação do Algoritmo da Divisão. Além disso, sabemos fatorar sem dificuldades em $\mathbb{Q}[x,y]/(p) \approx \mathbb{Q}[x]$, onde p é um polinômio linear sobre $\mathbb{Q}$ na variável y, de forma que o Levantamento de Hensel remove a restrição do algoritmo (2.1.1) à fatoração quando $F = \mathbb{Q}$.

Analisemos então a viabilidade de se criar uma versão do Levantamento de Hensel a polinômios com múltiplos fatores. Para tanto, sejam $f_1, ..., f_r$ fatores mônicos do polinômio f em $R[x]$ módulo m (isto é, $f \equiv cl_x(f) f_1 ... f_r \ mod \ m$). Supomos que o termo líder $cl_x(f)$ de f é invertível módulo m, com inverso denotado por a.

É possível arranjar facilmente os fatores mônicos ν de f módulo m em uma árvore binária τ de profundidade $d = \lceil log_2 r \rceil$, com folhas $f_1, ..., f_r$, raiz af e tal que cada nodo interno corresponde ao produto de dois filhos módulo m. O desenho abaixo ilustra como isso pode ser feito quando $r = 5$:



Além disso, para cada nodo interno $\nu \in R[x]$ com filhos g_ν e h_ν, vamos supor que conhecemos $s_\nu, t_\nu \in R[x]$ tais que $grau(s_\nu) < grau(h_\nu)$, $grau(t_\nu) < grau(g_\nu)$ e $s_\nu g_\nu + t_\nu h_\nu \equiv 1 \; mod \; m$ (em particular, isso implica que estamos supondo que f é livre de quadrados). Observe também que, no caso em que $R/(m)$ é um corpo, os elementos s_ν e t_ν podem ser obtidos pelo Algoritmo de Euclides Estendido. Uma árvore τ com tais propriedades é denominada árvore de fatoração módulo m.

O algoritmo abaixo calcula o Levantamento de Hensel de múltiplos fatores, que ergue uma árvore de fatoração módulo m a uma árvore de fatoração módulo m^l, onde l é um inteiro positivo arbitrário. A estrutura da árvore permanece inalterada durante o algoritmo, apenas os dados associados aos vértices variam.

Algoritmo 2.2.9. *Levantamento de Hensel de múltiplos fatores*

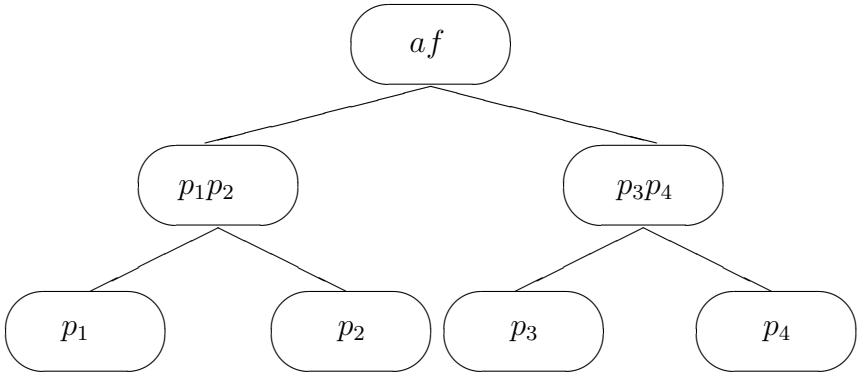
Entrada: *Um elemento m em um anel R comutativo e provido de unidade, $f \in R[x]$ de grau n, $a_0 \in R$ tal que $a_0 cl(f) \equiv 1 \; mod \; m$ e uma árvore de fatoração τ de f módulo m com raiz $a_0 f$ e r folhas.*

Saída: *Um inverso $a^\star \in R$ de $cl_x(f) \; mod \; m^l$ e uma árvore de fatoração $\tau^\star$ de f módulo m^l com raiz $a^\star f$ e tal que cada nodo $\nu^\star$ de $\tau^\star$ é congruente módulo m ao nodo ν correspondente de τ.*

1. $d \leftarrow \lceil log_2 l \rceil, \;\; \tau_0 \leftarrow \tau$
2. *para* $j = 1, 2, ..., d$ *faça*
3. $\{$*levantamento do inverso de* $cl_x(f)\}$
   calcula $a_j \in R$ *tal que* $a_j \equiv 2a_{j-1} - cl_x(f)a_{j-1}^2 \; mod \; m^{2^j}$
   $\tau_j \leftarrow \tau_{j-1}$
   substitui a raiz de τ_j *por* $a_j f$.
4. $\{$*levantamento da árvore*$\}$
   para cada nodo interno $\nu \in R[x]$ *de* τ_j, *procedendo da raiz às folhas, faça*
5. *utilize o algoritmo do Passo de Hensel (2.2.2) com m substituído por $m^{2^{j-1}}$ para erguer as congruências $\nu \equiv g_\nu h_\nu$ e $s_\nu g_\nu + t_\nu h_\nu \equiv 1$ módulo $m^{2^{j-1}}$ a congruências módulo m^{2^j}*
6. *devolve* a_d *e* τ_d.

Mais uma vez, mostraremos o funcionamento do algoritmo com nosso bem conhecido exemplo $f(x,y) = x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1$ em $F_2[x,y]$.:

Exemplo 2.2.10. *Consideremos o corpo $K = F_2[y]/(p)$, onde $p = y^4+y^3+y^2+y+1$, e vejamos f como polinômio em $K[x]$. Sobre esse corpo, $f = (y^3+y^2+y+1)p_1p_2p_3p_4$ para $p_1 = x + y^3 + y^2$, $p_2 = x^2 + y^2 + 1$, $p_3 = x + y^3 + y$ e $p_4 = x + y^2 + 1$. Uma árvore de fatoração módulo p é dada por*



Como p_1, p_2, p_3, p_4 são polinômios sobre um corpo, os elementos s_ν, t_ν correspondentes aos nodos da árvore foram obtidos pelo Algoritmo de Euclides Estendido. Além disso, $a = cl_x(f)^{-1} = y$. Vamos descrever como o algoritmo ergue essa árvore a uma árvore módulo p^2.

O primeiro passo é erguer o inverso do termo líder de f, para garantir que a árvore τ_1 contenha um polinômio mônico em sua raiz. Fazendo as contas, temos que o inverso de y^4 módulo p^2 é $a_1 \equiv 2a_0 - cl_x(f)a_0^2 \equiv 2y - y^4y^2 \equiv y^6$ mod p^2. A raiz de τ_1 será o polinômio y^6f, que é mônico módulo p^2.

Em seguida, erguemos os dois filhos da raiz. Para tanto, aplicamos o algoritmo do Passo de Hensel (2.2.2). Aqui, cabe uma observação: como alteramos a raiz de tal forma que ela permanecesse mônica após o levantamento, os seus filhos serão ambos mônicos quando aplicarmos o passo utilizando essa nova raiz como produto dos filhos. Note que isso não causa nenhum problema porque a nova raiz e

a antiga são congruentes módulo p. Dessa forma, obtemos uma árvore de fatoração módulo p^2 com a mesma estrutura, mas onde as entradas são:

$p_1p_2 = x^3 + (y^7 + y^5 + y^3 + 1)x^2 + (y^7 + y^5 + y^4 + y^3 + y^2 + y + 1)x + y^5 + y^4 + y^3 + y^2$
$p_3p_4 = x^2 + (y^7 + y^5 + y^3 + y)x + y^6 + 1$
$p_1 = x + y^7 + y^3$
$p_2 = x^2 + (y^5 + 1)x + y^6 + y^5 + y^2 + y$
$p_3 = x + y^3 + y$
$p_4 = x + y^2 + 1$

Provemos a validade do algoritmo e analisemos sua complexidade:

Teorema 2.2.11. *O algoritmo funciona. O número de operações em F é dado por $O(log\ rM(n)M(l\ grau_y m))$ se o grau em y de todas as entradas for inferior a $l\ grau_y m$.*

Demonstração

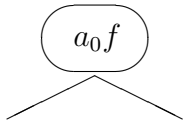
Inicialmente, demonstremos que a iteração no passo 3 está correta. Para tanto, veremos que, se $j \geq 1$ e a, b são tais que $ab \equiv 1\ mod\ m^{2^{j-1}}$ e $\hat{a} = 2a - ba^2\ mod\ m^{2^j}$, então $\hat{a}b \equiv 1\ mod\ m^{2^j}$. Mas $1 - \hat{a}b \equiv 1 - 2ab + ba^2b \equiv (1 - ab)^2\ mod\ m^{2^j}$. Como $1 - ab \equiv 0\ mod\ m^{2^{j-1}}$, existirá $r \in R$ tal que $1 - ab = rm^{2^{j-1}}$, logo $(1 - ab)^2 = r^2m^{2^j}$ e $\hat{a}b \equiv 1\ mod\ m^{2^j}$.

Por indução no número de gerações na árvore τ, demonstraremos que o levantamento da árvore de fatoração τ de f módulo m à arvore de fatoração τ_1 de f módulo m^2 é feito corretamente. Assim que tivermos estabelecido tal resultado, a validade do algoritmo seguirá aplicando-o indutivamente, pois o Passo de Hensel será novamente aplicado com m substituído por m^{2^j}, $j = 1, ..., d-1$. Obteremos ao final uma árvore de fatoração τ_d de f módulo m^{2^d}, que também será uma árvore de fatoração módulo m^l porque $l \leq 2^d$.

Demonstremos então a validade da afirmação do parágrafo anterior: se houver uma única geração, basta mostrar que $a_0 f \equiv a_1 f\ mod\ m$. Mas $a_1 \equiv 2a_0 -$

$cl_x(f)a_0^2$ módulo m^2 e, em particular, módulo m. Assim, $a_1 f - a_0 f = (a_1 - a_0)f \equiv (2a_0 - cl_x(f)a_0^2 - a_0)f \equiv a_0(1 - cl_x(f)a_0)f \equiv 0\ mod\ m$.

Suponha que τ tenha $k > 1$ gerações, isto é, τ tem a forma



Árvore A_1 Árvore A_2

onde A_1, A_2 têm no máximo $k - 1$ gerações.

Pela discussão da base de indução, obtém-se $a_1 f$ mônico módulo m^2 com $a_1 f \equiv a_0 f\ mod\ m$. Aplicando o passo de Hensel, obtemos $f_1^\star, f_2^\star \in F[x, y]$ tais que $f_1^\star \equiv f_1\ mod\ m$, $f_2^\star \equiv f_2\ mod\ m$, $a_1 f \equiv f_1^\star f_2^\star\ mod\ m^2$, $grau_x f_1 = grau_x f_1^\star$, $grau_x f_2 = grau_x f_2^\star$ e $f_2^\star$ é mônico.

Mas $grau_x(a_1 f) = grau_x(a_0 f) = grau_x f_1 + grau_x f_2 = grau_x f_1^\star + grau_x f_2^\star$ e ambos $a_1 f$ e $f_2^\star$ são mônicos módulo m^2. Logo, $f_1^\star$ é mônico módulo m^2 e é possível aplicar a hipótese de indução para as subárvores A_1 e A_2 com raízes f_1 e f_2 trocadas por $f_1^\star$ e $f_2^\star$, respectivamente, o que conclui a demonstração da validade do algoritmo.

Analisemos a sua complexidade. Nos três primeiros passos, devemos reduzir os coeficientes de f módulo m^{2^j} com respeito à variável x, e calcular o levantamento do elemento inverso do termo líder de f, ações essas que exigem $O(M(2^j grau_y m))$ operações. Mas esse custo poderá ser ignorado visto que os passos 4 e 5 são mais trabalhosos, pois envolvem contas semelhantes em polinômios em duas variáveis ao invés de uma. Na análise dos passos 4 e 5, o teorema (2.2.4) garante que a execução de cada passo 5, com j fixo, é da ordem de $O(M(grau\ \nu)M(2^j m))$, pois temos a cota $A = 2^j$. A árvore τ_j conta com $\lceil log\ r \rceil$ gerações. Além disso, para uma dada geração, a soma dos graus em x dos polinômios em cada um dos nodos é limitada por n. Logo, o custo total para essa geração será limitado por $O(M(n)M(2^j grau_y m))$ pelo fato de M ser subaditiva (ou seja, $M(m + n) <$

$M(m) + M(n)$ para quaisquer $m, n \in \mathbb{N}$). Para j fixo, o custo total dos passos 4 e 5 é $O(log\ rM(n)M(2^j grau_y m))$. Novamente utilizando a subaditividade, somamos essas cotas de $j = 1$ a d e obtemos $O(log\ rM(n)M(2^{d+1} grau_y m)) = O(log\ rM(n)M(ldeg_y m))$. □

Mas, agora que vimos como erguer a fatoração de um polinômio em duas variáveis módulo um primo pequeno a fatorações módulo potências arbitrárias desse primo, podemos facilmente escrever um algoritmo de fatoração. A versão abaixo foi adaptada de um algoritmo similar para fatoração de polinômios em uma variável sobre o anel dos inteiros, inicialmente proposto por Zassenhaus [Zassenhaus, 1969].

Algoritmo 2.2.12. *Fatoração de polinômios por potências de primos*

Entrada: *Um polinômio primitivo f em $R[x] = F[x, y]$, onde $R = F[y]$ para um corpo F com pelo menos $4nd$ elementos e fatoração efetiva para polinômios em uma variável. Aqui, $n = grau_x f \geq 1$, $d = grau_y f$, e $mdc(f, \frac{\partial f}{\partial x}) = 1$ em $F(y)[x]$.*

Saída: *Os fatores irredutíveis $\{f_1, ..., f_k\} \subseteq F[x, y]$ de f.*

1. *se $n = 1$ então devolva f*
   $b \leftarrow cl_x(f)$
   escolha $U \subseteq F$ de cardinalidade $\sharp U = 4nd$
2. *repita*
   escolha aleatoriamente $u \in U$, $\bar{f} \leftarrow f(x, u)$
   até que $b(u) \neq 0$ e $mdc(\bar{f}, \frac{\partial \bar{f}}{\partial x}) = 1$ em $F[x]$.
   $l \leftarrow d + 1 + grau(b)$
3. {*Fatoração modular*}
   utilize um algoritmo de fatoração em uma variável para calcular
   $f \equiv bh_1...h_r\ mod\ (y - u)$ em $(F[y]/(y - u))[x] \simeq F[x]$,
   para certos polinômios mônicos irreduíveis $h_1, ..., h_r$ em $F[x]$.
4. {*Levantamento de Hensel*}
   $a \leftarrow b(u)^{-1}$
   utilize o Algoritmo de Euclides Estendido para calcular uma árvore de fatoração

de f módulo $y-u$ em $F[x]$ com folhas $h_1, ..., h_r$.

utilize o Levantamento de Hensel de Múltiplos Fatores para calcular uma fatoração $f \equiv bg_1...g_r \ mod \ (y-u)^l$, para polinômios $g_1, ...g_r$ em $F[x,y]$ que são mônicos com respeito a x e tais que $grau_y g_i < l$ e $g_i(x,u) = h_i$, $1 \leq i \leq r$.

5. {*Inicialização do conjunto de índices T de fatores modulares ainda não considerados, do conjunto G de fatores encontrados, e do polinômio $f^\star$ a ser fatorado*}
   $T \leftarrow \{1, 2, ..., r\}$, $s \leftarrow 1$, $G \leftarrow \emptyset$, $f^\star \leftarrow f$
6. {*Combinação de fatores*}
   enquanto $2s \leq \sharp T$ *faça*
7. *para todos subconjuntos $S \subseteq T$ de cardinalidade $\sharp S = s$ faça*
8. *calcule $g^\star$, $h^\star \in F[x,y]$ com grau em y inferior a l satisfazendo $g^\star \equiv b \prod_{i \in S} g_i \ mod \ p$ e $h^\star \equiv b \prod_{i \in T \backslash S} g_i \ mod \ p$*
9. *se $grau_y(g^\star h^\star) = grau_y(bf^\star)$ então*
   $T \leftarrow T \backslash S$, $G \leftarrow G \cup pp_x(g^\star)$,
   $f^\star \leftarrow pp_x(h^\star), b \leftarrow cl_x(f^\star)$
   interrompa o laço 7 e vá a 6.
10. $s \leftarrow s + 1$
11. *devolva* $G \cup \{f^\star\}$

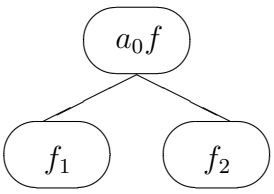
Apliquemos esse algoritmo a um exemplo. Infelizmente, a restrição no número de elementos no corpo base impede que utilizemos nosso tradicional polinômio.

Exemplo 2.2.13. *Consideremos o polinômio*

$$f(x,y) = (y+54)x^5 + yx^4 + (y^3+54y^2+4y+33)x^3 + (y^3+9y+3)x^2 + 5y^3 + 3y^2 + 20y^3 + 12$$

em $F_{61}[x,y]$. Note que $n = grau_x f = 5$ e $d = grau_y(f) = 3$. Logo, $4nd = 60$ e o corpo F_{61} tem elementos suficientes para que o algoritmo possa ser aplicado. Além disso, $mdc(f, \frac{\partial f}{\partial x}) = 1$, de forma que f é primitivo como polinômio na variável x sobre o corpo $F_{61}(y)$. Portanto, f é um polinômio que satisfaz as condições de entrada do algoritmo.

No primeiro passo, definimos $b = y + 54$ *e escolhemos* $U \subset F_{61}$ *com* 60 *elementos, digamos* $U = \{1, 2, ..., 60\}$. *Em seguida, escolhemos aleatoriamente um elemento* $u \in U$. *Suponhamos que* $u = 7$ *tenha sido escolhido. Infelizmente, essa escolha é inadequada, pois* $b(7) = 7 + 54 \equiv 0 \ mod\ 61$. *Escolhamos um segundo* u, *digamos* $u = 13$. *Logo,* $b(13) = 13 + 54 \equiv 6 \ mod\ 61$ *e* $mdc(f(x, 13), \frac{\partial f}{\partial x}(x, 13)) = mdc(6x^5 + 13x^4 + x^3 + 60x^2 + 52, 30x^4 + 52x^3 + 3x^2 + 59x) = 1$ *em* $F_{61}[x]$, *o que caracteriza uma boa escolha. Calculamos* $l = 1 + d + grau\ b = 5$ *e dirigimo-nos ao passo* 3. *Obtém-se a fatoração* $f(x, 13) = 6(x^2 + 51)(x^3 + 53x^2 + 52)$ *em* $F_{61}[x]$, *que é equivalente à fatoração* $f(x, y) = 6(x^2+51)(x^3+53x^2+52)$ *em* $(F_{61}[y]/(y+48))[x]$ *e nos dá a árvore de fatoração*



onde

$a_0 = 6^{-1} \equiv 51 \ mod\ 61$
$f_1 = x^2 + 51$
$f_2 = x^3 + 53x^2 + 52$
$s = 57x^2 + 33x + 13, \ \ t = 4x + 60,$ *com* $sf_1 + tf_2 = 1$

Alcançamos o passo 4, *quando o Passo de Hensel deve ser aplicado. Note que o levantamento deve ser feito* $\lceil log\ l \rceil = \lceil log\ 5 \rceil = 3$ *vezes. Fazendo as contas, chegamos a uma árvore de fatoração módulo* $(y+48)^{2^3} = y^8 + 18y^7 + 35y^6 + 5y^5 + 56y^4 + 52y^3 + 28y^2 + 18y + 47$ *com a mesma estrutura da árvore acima e entradas*

$a_3 = 45y^7 + 27y^6 + 56y^5 + 7y^4 + 7y^3 + 10y^2 + 49y + 55$
$f_1 = x^2 + y^2 + 4$
$f_2 = x^3 + (10y^7 + 6y^6 + 26y^5 + 49y^4 + 49y^3 + 9y^2 + 38y + 20)x^2 +$

$$
\begin{aligned}
& 2y^7 + 50y^6 + 54y^5 + 22y^4 + 22y^3 + 14y^2 + 32y + 21 \\
s = & (y^7 + 27y^6 + 60y^5 + 4y^4 + 5y^3 + 37y + 14)x^2 + \\
& (47y^7 + 34y^6 + 5y^5 + 36y^4 + 51y^3 + 10y^2 + 21y + 26)x + \\
& 7y^7 + 58y^6 + 48y^5 + 29y^4 + 53y^3 + 19y^2 + 54y + 36 \\
t = & (60y^7 + 34y^6 + y^5 + 57y^4 + 56y^3 + 24y + 47)x + \\
& 52y^7 + 10y^6 + 11y^5 + 21y^4 + 46y^3 + 31y^2 + 58y + 48
\end{aligned}
$$

Agora, recuperaremos a fatoração desejada a partir da fatoração encontrada $f(x,y) = (y+54)(x^2+y^2+4)(x^3+(10y^7+6y^6+26y^5+49y^4+49y^3+9y^2+38y+20)x^2+2y^7+50y^6+54y^5+22y^4+22y^3+14y^2+32y+21)$ *em* $(F_{61}[y]/(y+48)^{2^3})[x]$. *Isso será feito seguindo o procedimento do algoritmo (2.1.1). Nesse, exemplo particular, tivemos sorte de que a fatoração módulo* $y+48$ *não quebrou nenhum fator irredutível de* f *sobre* $F_{61}[x,y]$ *em fatores menores. Assim, nenhum teste falhará e recuperaremos facilmente os fatores irredutíveis* x^2+y^2+4 *e* $(y+54)x^3+yx^2+5y+3$ *de* f *em* $F_{61}[x,y]$.

Vejamos agora a validade do algoritmo.

Teorema 2.2.14. *O algoritmo acima devolve o resultado desejado. O custo esperado para cada passagem pelo passo* 2 *é* $O(nd + M(n)log\ n)$ *operações aritméticas em* F, *e o passo* 4 *leva* $O(M(n)log(n)M(d))$ *operações. O número de operações sobre o corpo para uma iteração dos passos* 8 *e* 9 *é* $O(M(d)(nlog\ d + M(n)log\ n))$, *e há no máximo* 2^{n+1} *iterações. Se* $F = F_q$ *é um corpo finito com* q *elementos, então o número esperado de operações em* F_q *no passo* 3 *é* $O(M(n^2)log\ n + M(n)log(n)log(q))$.

Demonstração

Comecemos pela validade. Vejamos que encontraremos $u \in U$ satisfazendo as condições requeridas no passo 2. Lembremos que $b \in F[y]$ é um polinômio com $grau\ b = grau\ cl_x(f) \leq grau_y f = d$. Como b é um polinômio em uma variável sobre um corpo, ele possui no máximo d raízes. Por outro lado, do fato que

$mdc(f, \frac{\partial f}{\partial x}) = 1$ em $F(y)[x]$, existem $s, t \in F(y)$ tais que $sf + t\frac{\partial f}{\partial x} = 1$. O seguinte resultado, cuja demonstração pode ser encontrada em [von zur Gathen e Gerhard, 1999], caracteriza melhor tais elementos s e t:

Resultado: Sejam F um corpo, $g, h \in F[x, y]$ com $n = grau_x(g) \geq grau_x(h) = m$ e $grau_y(g),\ grau_y(h) \leq d$. Os resultados intermediários do Algoritmo de Euclides Estendido para g e h em $F(y)[x]$ podem ser escritos com numeradores e denominadores com grau em y limitado por $(n + m)d$.

Logo, poderemos escrever $s = p_0(y)/q_0(y),\ t = p_1(y)/q_1(y)$, onde o grau em y de $p_0, q_0, p_1, q_1 \in F[y]$ é limitado por $(n + n - 1)d = (2n - 1)d$. Mas $p_0 f + p_1 \frac{\partial f}{\partial x} = q_0 q_1$, com $grau_y(q_0 q_1) \leq 4nd - 2d$. Portanto, o máximo divisor comum de f e $\frac{\partial f}{\partial x}$ módulo m não é um elemento invertível em $F[y]/(m)$ para no máximo $4nd - 2d$ elementos de F. Assim, existem no máximo $4nd - 2d + d = 4nd - d$ elementos de F que não satisfazem alguma das condições de 2. Como $d \geq 1$, segue que $4nd - d < 4nd$, ou seja, encontraremos um elemento u como procuramos.

Mas supomos conhecida a fatoração em uma variável, logo o passo 3 é realizado com sucesso. Sabemos também que podemos encontrar polinômios $g_1, ..., g_r \in F[x, y]$ mônicos com respeito a x tais que $f \equiv b g_1 ... g_r\ mod\ (y - u)^l$, $grau_y(g_1) < l$ e $g_i \equiv h_i\ mod\ (y - u)$. Mas $g_i(x, y) \equiv g_i(x, u)\ mod\ (y - u)$ pelo Teorema do Resto, logo $g_i(x, u) \equiv h_i(x)\ mod\ (y - u)$ e, como nenhum deles depende da variável y, $g_i(x, u) = h_i(x)$.

A seqüência do algoritmo simplesmente recupera os fatores em $F[x, y]$ da fatoração módulo $(y - u)^l$, que, pela definição de l, tem grau suficientemente grande para que isso seja feito, conforme se verifica seguindo a demonstração da validade do algoritmo (2.1.1).

Vejamos agora a análise do algoritmo. O custo para cada passagem pelo passo 2 é de $O(nd)$ operações aritméticas em F para avaliar o polinômio f em $y = u$ (isso também é uma cota para as avaliações de b e $\frac{\partial f}{\partial x}$ em $y = u$) e $O(M(n)log\ n)$

para calcular o máximo divisor comum. Logo, a complexidade de cada passagem é $O(nd + M(n)log\ n)$. Note que o número de passagens é limitado por $4nd$.

A estimativa para o passo 4 vem do teorema (2.2.11), donde o número de operações é dado por $O(M(n)log\ rM(lgrau_y(y-u))$. É claro que $r \leq n$ e $l \leq 2d+1$, isto é, essa estimativa pode ser reescrita como $O(M(n)log\ nM(d))$. Deve-se somar a isso o custo das sucessivas aplicações do Algoritmo de Euclides Estendido, que soma $O(M(n)log\ n\ log\ n)$.

O custo envolvido nos passos 8 e 9, bem como o número de iterações, pode ser estabelecido de forma análoga ao que foi feito no teorema (2.1.3). A cota para o passo 3 vem dos algoritmos para fatoração em uma variável sobre corpos finitos. □

Observação

Quando $F = F_q$ é um corpo finito pequeno, temos problemas no passo 1. Há diversas maneiras de transpô-los. Podemos recorrer a um algoritmo para primos grandes, conforme vimos anteriormente, mas isso acarreta um maior custo no estágio de fatoração modular. Também é viável fatorar f módulo um elemento irredutível $m \in F_q[x]$ de grau $O(log\ nd)$, ao invés de módulo $(y-u)$, e erguer essa fatoração a uma potência suficientemente grande de m no passo 4. Ou ainda, pode-se realizar uma extensão de corpos de grau $O(log\ nd)$ e aplicar o presente algoritmo a f sobre esse corpo maior. Porém, devemos observar que fatores irredutíveis de f em $F_q[x,y]$ são passíveis de decomposição em fatores menores sobre essa extensão.

Adaptaremos o nosso algoritmo a nosso clássico exemplo.

Exemplo 2.2.15. *O polinômio que desejávamos fatorar era*

$$f(x,y) = x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1$$

em $F_2[x,y]$. *Logo,* $n = grau_x f = 5 = grau_y f = d$.

Lembre que, como havíamos comentado no exemplo anterior, não se pode aplicar o algoritmo diretamente para f, *pois os coeficientes de* f *estão em* F_2,

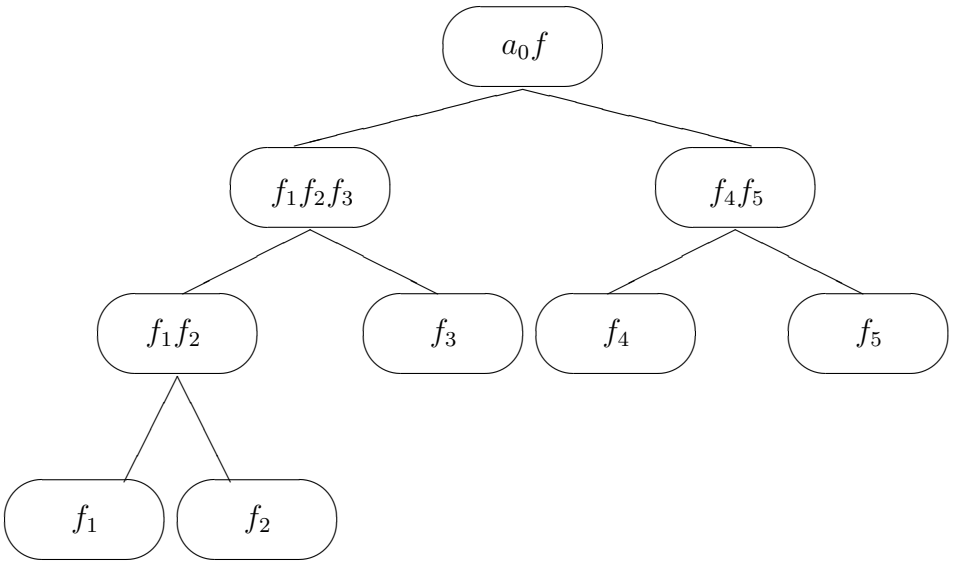
que conta com apenas dois elementos. Então, procederemos como na observação acima e, ao invés de trabalharmos módulo $y - u$*, para algum* $u \in F_2$*, fatoraremos módulo* p*, para um polinômio* p *irredutível de grau quatro. Um candidato natural seria* $p = x^4+x^3+x^2+x+1$*, que já foi utilizado em exemplos anteriores. Entretanto, a fatoração completa de* f *em* $(F_2[y]/(y^4 + y^3 + y^2 + y + 1))[x]$ *é dada por*

$$(x + y^3 + y^2)(x + y + 1)^2(x + y^3 + y)(x + y^2 + 1),$$

ou seja, f *mod* p *não é livre de quadrados e, portanto, não é uma boa escolha. Mas* $p = y^4+y+1$ *resulta em uma fatoração satisfatória. Fazendo as contas, verificamos que*

$$f = (x + y)(x + y + 1)(x + y^3)(x + 1)(x + y^3 + y + 1)$$

em $(F[y]/(y^4 + y + 1))[x]$*. Como* $grau_y(f) = 5$*, sabemos que, se erguermos essa fatoração a uma fatoração módulo* $(y^4 + y + 1)^4$*, poderemos recuperar os fatores originais. Essa cota vem do seguinte fato: o grau do polinômio na congruência ao final do levantamento deve ser* $l = n + grau\ b + 1 = 10$*, pelo mesmo motivo de essa ser a cota quando partimos de polinômios da forma* $y - u$*. Como partimos de um polinômio de grau igual a* 4*, devemos realizar* $\lceil log\ (\frac{10}{4}) \rceil = 2$ *levantamentos. Seja então a árvore de fatoração*



$a_0 = y^3 + y^2 + y$

$f_1 f_2 f_3 = x^3 + (y^3+1)x^2 + (y^3+y^2+y)x + y^2 + 1$

$f_1 f_2 = x^2 + x + y^2 + y$

$f_4 f_5 = x^2 + (y^3+y)x + y^3 + y + 1$

$f_1 = x + y$

$f_2 = x + y + 1$

$f_3 = x + y^3$

$f_4 = x + 1$

$f_5 = x + y^3 + y + 1$

Após o levantamento de Hensel, obtemos uma árvore de fatoração análoga (módulo $y^{16} + y^4 + 1$*) em que*

$a_2 = y^{12} + 1$

$f_1 f_2 f_3 = x^3 + (y^{15} + y^7 + y + 1)x^2 + (y^{15} + y^{10} + y^8 + y^7 + y^4 + y^2 + 1)x +$
$y^{11} + y^{10} + y^3 + y^2$

$f_1 f_2 = x^2 + (y^{15} + y^7 + y^3 + y + 1)x + y^{15} + y^8 + y^7 + y^3 + 1$

$f_4 f_5 = x^2 + (y^{15} + y^7)x + y^{10} + y^6$

$f_1 = x + y^{15} + y^7 + y^3$

$f_2 = x + y + 1$

$f_3 = x + y^3$

$f_4 = x + y^{15}$

$f_5 = x + y^7$

Devemos recombinar os fatores, o que será feito por tentativas. Teremos menos sorte do que no último exemplo e algumas combinações falharão até obtermos a fatoração $f = (x + y + 1)(x^4y^4 + xy + 1)$.

Portanto, obtivemos um algoritmo que aprimora nossa tentativa inicial, pois fatora em estruturas menores e em seguida ergue esses fatores, o que acarreta

uma sensível redução de custo computacional e, principalmente, permite que calculemos a fatoração de polinômios em duas variáveis com coeficientes racionais. Por outro lado, o problema da combinação dos fatores obtidos modularmente para reconstruir os fatores procurados não foi enfrentado por ora, de forma que esse algoritmo ainda recorre à combinação por tentativas e, conseqüentemente, não resolve nosso problema em tempo polinomial no pior caso.

Isso justifica o fato de que essa dificuldade venha a ser alvo de nosso estudo, cuja superação [Lenstra et al., 1982] foi um marco na história da Álgebra Computacional. O ingrediente técnico principal, os vetores curtos em reticulados, serão assunto do que vem a seguir.

2.3 Reticulados e Redução de Base

Os métodos que discutiremos nessa subseção têm suas raízes no estudo de aspectos computacionais da Geometria de Números, teoria matemática que foi introduzida por Hermann Minkowski por volta de 1890 e que é descrita em [Minkowski, 1910]. Primordialmente, desenvolveu-se uma teoria para números inteiros, que foi com o tempo adaptada para o nosso problema de fatoração em duas variáveis sobre corpos. Iniciemos pela definição clássica:

Definição 2.3.1. *Sejam $n \in \mathbb{N}$ e $f_1, ..., f_n \in \mathbb{R}^n$, com $f_i = (f_{i1}, ..., f_{in})$. O reticulado ou $\mathbb{Z}$-módulo gerado por $f_1, ..., f_n$ é o conjunto*

$$L = \sum_{i=1}^{n} \mathbb{Z} f_i = \{\sum_{i=1}^{n} r_i f_i;\ r_1, ..., r_n \in \mathbb{Z}\}.$$

O famoso algoritmo de Lenstra, Lenstra e Lóvasz [Lenstra et al., 1982] resolveu o problema da recuperação de fatores de um polinômio $f \in \mathbb{Z}[x]$ a partir de fatores conhecidos de f módulo m, para algum $m \in \mathbb{Z}_+$, recorrendo a bases de tamanho "pequeno" com relação a uma determinada norma. Para uma definição

precisa de vetor pequeno em um reticulado, para uma análise detalhada do algoritmo LLL para redução de base, que envolve por exemplo ortogonalização de Gram-Schmidt, e para a conexão da redução de base com a fatoração de polinômios, recomendam-se o trabalho original [Lenstra et al., 1982] ou mesmo o livro de J. von zur Gathen e J. Gerhard [von zur Gathen e Gerhard, 1999].

Com base na semelhança entre os problemas de fatoração de polinômios sobre $\mathbb{Z}[x]$ e sobre $F[x, y]$, insistentemente repetida no presente capítulo, podemos esperar idéias semelhantes possam ser adaptadas ao anel $F[x, y]$. Define-se um reticulado em $F[y]$ essencialmente da mesma maneira que em (2.3.1), substituindo $R = F[y]$ e $\mathbb{Z}$-módulos por $F[y]$-módulos. Assim como na teoria sobre $\mathbb{Z}$, conseguiremos calcular a redução de base em tempo polinomial e relacioná-la com a fatoração de polinômios em $F[x, y]$, mais precisamente, com a recuperação em tempo polinomial dos fatores em $F[x, y]$ dada uma fatoração módulo $m \in F[y]$.

De fato, a redução de base é muito mais simples sobre $F[y]$ do que sobre $\mathbb{Z}$. Por exemplo, sempre encontraremos um vetor de comprimento mínimo em um reticulado m-dimensional sobre $F[y]^n$ em tempo polinomial, o que provavelmente não é verdade para $\mathbb{Z}$-módulos, onde esse problema é NP completo. O algoritmo de fatoração desenvolvido a partir desse resultado nada mais será do que a redução em tempo polinomial da fatoração de polinômios em duas variáveis à de polinômios em uma variável sobre o corpo F.

Sejam, então, um corpo F, $R = F[y]$ e $n \in N$. A norma do máximo de um vetor $f = (f_1, ..., f_n) \in R^n$ é dada por $\|f\| = \|f\|_\infty = max_{1 \leq i \leq n} grau f_i$. Para vetores $f_1, ..., f_m$ em R^n que são linearmente independentes sobre $F(y)$, o corpo de frações de R, o R-módulo ou reticulado gerado por $f_1, ..., f_m$ é $M = \sum_{i=1}^{m} Rf_i$ e diz-se que $f_1, ..., f_m$ formam uma base para M.

Definição 2.3.2. *Sejam $f_1, .., f_m \in R^n$ vetores linearmente independentes sobre $F(y)$, com $f_i = (f_{i1}, ..., f_{in})$, $1 \leq i \leq m$. Dizemos que a seqüência $(f_1, ..., f_m)$ é reduzida se:*

(i) $\|f_1\| \leq \|f_2\| \leq ... \leq \|f_m\|$

(ii) $grau f_{ij} \leq grau f_{ii}$, $1 \leq j \leq n$, *com desigualdade estrita para* $j < i$, $i = 1, 2, ..., m$

Em particular, $\|f_i\| = grau f_{ii}$, $1 \leq i \leq m$.

Conforme mencionamos acima, uma seqüência reduzida nos fornece um vetor de comprimento mínimo contido em um determinado reticulado, e isso será conseqüência imediata da proposição abaixo:

Proposição 2.3.3. *Seja M o reticulado gerado pela seqüência reduzida $f_1, ..., f_m$ em R^n. Então $\|f\| \geq \|f_1\|$, $\forall f \in M \backslash \{0\}$.*

Demonstração

Sejam $f \in M\backslash\{0\}$ e $a_1, ..., a_m \in R$ tais que $f = \sum_{i=1}^{m} a_i f_i$. Como f não é nulo, $L = max\{grau\ a_k f_k;\ k = 1, ..., n\}$ está bem definido. Consideremos $\Sigma = \{k \in \{1, 2, ..., m\};\ grau\ a_k f_k = L\}$ e tomemos k_0 mínimo em Σ.

Seja $j \in \{1, ..., m\}\backslash\{k_0\}$. Se $j \notin \Sigma$, $grau\ a_{k_0} f_{k_0 k_0} > grau\ a_j f_{jj} \geq grau\ a_j f_{k_0 j}$, pois o conjunto é reduzido. Agora, se $j \in \Sigma$, $j > k_0$ e $grau\ a_{k_0} f_{k_0 k_0} = grau\ a_j f_{jj} > grau\ a_j f_{k_0 j}$, também pela redutibilidade do conjunto.

Conclui-se que o grau do termo líder de $a_{k_0} f_{k_0 k_0}$ é estritamente maior que o do termo líder de $a_j f_{k_0 j}$, para todo $j \neq k_0$. Por isso, a k_0-ésima coordenada de f, dada por $\sum_{i=1}^{m} a_i f_{k_0 i}$ tem termo líder de grau $grau\ a_{k_0} f_{k_0 k_0} \geq grau\ a_{k_0} f_{11} \geq \|f_1\|$, já que $a_{k_0} \neq 0$. Logo, $\|f\| \geq \|f_1\|$.□

O seguinte algoritmo, de von zur Gathen [von zur Gathen, 1984], determina uma seqüência reduzida associada a um R-módulo:

Algoritmo 2.3.4. *Redução de Base para Polinômios*

Entrada: *Vetores linha linearmente independentes* $f_1, ..., f_m \in R^n$, *onde* $R = F[y]$ *para certo corpo* F, *e* $\|f_i\| < d$, $1 \leq i \leq m$.

Saída: *Vetores linha* $g_1, ..., g_m$ *em* R^n *e uma matriz de permutação* $A \in R^{n\times n}$ *tal que* $(g_1, ..., g_m)$ *é uma seqüência reduzida e* $g_1A, ..., g_mA$ *formam uma base de* $M = \sum_{i=1}^{m} Rf_i$.

1. *Determine* $g_1, ..., g_m$ *tais que* $\{g_1, ..., g_m\} = \{f_1, ..., f_m\}$ *e* $\|g_i\| \leq \|g_{i+1}\|$, $i = 1, 2, ..., m-1$
   $A \leftarrow I_{n\times n}$, $k \leftarrow 1$.
2. *enquanto* $k \leq m$ *faça*
3. $\{(g_1, ..., g_k)$ *é seqüência reduzida e* $\|g_i\| \leq \|g_{i+1}\|$, *para* $1 \leq i < m\}$
   $u \leftarrow \|g_k\|$
4. *para* $i = 1, ..., k-1$ *faça*
5. $q \leftarrow g_{ki}$ *quo* g_{ii}, $g_k \leftarrow g_k - qg_i$
6. *se* $\|g_k\| < u$
   então
   $r \leftarrow min\{i;\ i = k$ *ou* $(1 \leq i < k$ *e* $\|g_i\| > \|g_k\|)\}$
   substitua $g_r, ..., g_{k-1}, g_k$ *por* $g_k, g_r, ..., g_{k-1}$
   $k \leftarrow r$.
   senão
7. $l \leftarrow min\{k \leq j \leq n;\ graug_{kj} = u\}$
   seja B *em* $R^{n\times n}$ *a matriz de*
   permutação para troca das colunas k *e* l.
   para $i = 1, 2, ..., m$ *faça*
   $g_i \leftarrow g_iB$
   $A \leftarrow BA$
   $k \leftarrow k + 1$
8. *devolva* $g_1, ..., g_m$ *e* A

Nada melhor do que um exemplo para entendermos o funcionamento desse algoritmo.

Exemplo 2.3.5. *Aplicaremos o algoritmo de redução de base acima para obtermos uma seqüência reduzida para o reticulado gerado pelos vetores* $f_1 = (y^2+1, y^3+2y, y+4, 0)$, $f_2 = (y^5+3y+1, y, 0, y^2+3y)$, $f_3 = (y^4+3y^3+y, y^2+2, y, y+1)$ *em* $F_5[y]^4$, *lembrando que* $F_5 = GF(5) = \mathbb{Z}_5$. *Não é difícil de verificar que eles são linearmente independentes sobre* $F_5(y)$.

Iniciamos definindo a seqüência (g_1, g_2, g_3) *com* $g_1 = f_1 = (y^2+1, y^3+2y, y+4, 0)$, $g_2 = f_3 = (y^4+3y^3+y, y^2+2, y, y+1)$, $g_3 = f_2 = (y^5+3y+1, y, 0, y^2+3y)$, *de tal forma que* $\|g_1\| \leq \|g_2\| \leq \|g_3\|$. *Definem-se* A *a matriz identidade* $I_{4\times 4}$ *e* $k = 1$.

Na primeira passagem pelo passo 2, $u = \|g_1\| = 3$. *O laço do passo* 4 *não é realizado e o teste do passo* 6 *falha. Logo, calculamos* $l = min\{1 \leq j \leq 4;\ graug_{1j} = 3\} = 2$ *e definimos* B *a matriz* 4×4 *que permuta as duas primeiras colunas. Assim,* $g_1 = (y^3+2y, y^2+1, y+4, 0)$, $g_2 = (y^2+2, y^4+3y^3+y, y, y+1)$, $g_3 = (y, y^5+3y+1, 0, y^2+3y)$, A *é a matriz de permutação das duas primeiras colunas e* $k = 2$.

Retornamos ao passo 2 *com* $u = \|g_2\| = 4$. *O laço do passo* 4 *é feito uma única vez e resulta em* $q = 0$, *de forma que não há mudanças. O teste* 6 *falha e o passo* 7 *não causa qualquer alteração a menos de um incremento em* k. *Agora,* $k = 3$, $u = \|g_3\| = 5$. *O laço* 2 *é realizado duas vezes. Na primeira, vem* $q = 0$ *e na segunda,* $q = quo(g_{32}, g_{22}) = quo(y^5+3y+1, y^4+3y^3+y) = y+2$. *Calculamos* $g_3 = g_3 - qg_2 = (4y^3+3y^2+4y+1, 4y^3+4y^2+y+1, 4y^2+3y, 3)$. *Como* $\|g_3\| = 3 < 5 = u$, *o teste do passo* 6 *tem resposta afirmativa e* $r = min\{i;\ i = 3$ *ou* $(1 \leq i < 3$ *e* $\|g_i\| > \|g_3\|)\} = 3$. *Substituimos então* g_1, g_2, g_3 *por* g_1, g_3, g_2 *e* $k = 2$. *Retornamos ao passo* 2 *e obtemos* $u = \|g_2\| = 3$. *Aplicando o laço do passo* 4, *obtêm-se* $q = quo(g_{21}, g_{11}) = quo(4y^3+3y^2+4y+1, y^3+2y) = 4$ *e* $g_2 = g_2 - qg_1 = (3y^2+y+1, 4y^3+y+2, 4y^2+4y+4, 3)$. *Como* $\|g_2\| = 3 = u$, *dirigimo-nos ao passo* 7, *onde apenas* k *será incrementado a* $k = 3$. *Temos* $u =$

$\|g_3\| = 4$ *e realizamos o laço em* 4. *Na primeira passagem,* $q = 0$, *na segunda,* $q = quo(g_{32}, g_{22}) = quo(y^4 + 3y^3 + y, 4y^3 + y + 2) = y + 4$ *e* $g_3 = g_3 - qg_2 = (3y^3 + y^2 + 4y, y^2 + y + 1, 4y^3 + y^2 + 2y + 2, 4y)$. *Segue que* $\|g_3\| = 3 < 4 = u$. *Como* $r = min\{i;\ i = 3\ ou\ (1 \leq i < 3\ e\ \|g_i\| > \|g_3\|)\} = 3$, *obtemos* $k = 3$ *e retornamos ao passo* 2, *agora com* $u = 3$. *A primeira passagem pelo laço* 2 *gera* $q = quo(g_{31}, g_{11}) = quo(3y^3+y^2+4y+3, y^3+2y) = 3$ *e* $g_3 = g_3 - qg_1 = (y^2+3y, 3y^2+y+3, 4y^3+y^2+4y, 4y)$. *A segunda passagem tem* $q = 0$ *e a condição em* 6 *é falsa. No passo* 7, *vem que* $l = 3$, *ou seja, não há alteração outra que um incremento em* k. *Agora* $k = 4$ *e o laço* 2 *é interrompido. O algoritmo retorna a seqüência reduzida* $((y^3+2y, y^2+1, y+4, 0), (3y^2 + y + 1, 4y^3 + y + 2, 4y^2 + 4y + 4, 3), (y^2 + 3y, 3y^2 + y + 3, 4y^3 + y^2 + 4y, 4y)$ *e a matriz* A.

Note que multiplicando os elementos da seqüência à direita por A, *vem a base* $((y^2 + 1, y^3 + 2y, y + 4, 0), (4y^3 + y^2, 3y^2 + y + 1, 4y^2 + 4y + 4, 3), (3y^2 + y + 3, y^2 + 3y, 4y^3 + y^2 + 4y, 4y)$ *para* L. *De fato, se denotarmos essa base por* g_1^*, g_2^*, g_3^*, *teremos* $f_1 = g_1^*$, $f_2 = 3yg_1^* + 4y^2g_2^* + (4y + 2)g_3^*$ *e* $f_3 = 3g_1^* + (4y + 2)g_2^* + g_3^*$.

A demonstração da validade do algoritmo será relativamente laboriosa. Inicialmente, estabeleceremos que o algoritmo fornece a resposta esperada supondo que ele atinja o passo 8. Em seguida, mostraremos que o passo 8 é de fato atingido.

A primeira proposição garante que sempre contamos com uma base para o reticulado em questão:

Proposição 2.3.6. *A igualdade* $M = \sum_{i=1}^{m} Rg_iA$ *permanece válida no decorrer do algoritmo. Em particular, os vetores* g_i *nunca são nulos.*

Demonstração

Para verificar esse resultado, mostraremos que a igualdade acima se verifica sempre que o algoritmo alcança o passo 2. Na primeira passagem por 2, $A = I_{n\times n}$ e $\{g_1, ..., g_m\} = \{f_1, ..., f_m\}$, de forma que $\sum_{i=1}^{m} Rg_iA = \sum_{i=1}^{m} Rf_i = M$.

Suponhamos que $\sum_{i=1}^{m} Rg_iA = M$ após determinada passagem por 2. Se $k < 2$, o passo 4 não será realizado, logo suporemos $k \geq 2$. Seja, para cada $i = 1, ..., k-1$, $q_i = g_{ki}$ *quo* g_{ii}. Após o final do laço, g'_k, o novo estado da variável g_k, será dado por $g'_k = g_k - \sum_{i=1}^{k} q_i g_i \neq 0$, pois o coeficiente de g_k é igual a 1 e $g_1, ..., g_k$ são linearmente independentes sobre $F(y)$. Mas, a igualdade acima implica $g'_k A \in \sum_{i=1}^{m} Rg_iA$ e $g_kA \in \sum_{i=1}^{k-1} Rg_iA + Rg'_kA$, de forma que $M = \sum_{i=1}^{m} Rg_iA = \sum_{1 \leq i \leq m,\ i \neq k} Rg_iA + Rg'_kA$.

Se a condição do passo 6 for verdadeira, nosso resultado será verificado, pois haverá no máximo uma mudança na ordem dos g_i's na lista. Já se a condição for falsa, definem-se $g'_i = g_iB$ e $A' = BA$, onde B é a matriz $n \times n$ de permutação das colunas l e k. Logo, $B^2 = I_{n \times n}$, e $M = \sum_{i=1}^{m} Rg_iA = \sum_{i=1}^{m} Rg_iB^2A = \sum_{i=1}^{m} R(g_iB)(BA) = \sum_{i=1}^{m} Rg'_iA'$, o que conclui a demonstração. □

A proposição acima estabelece uma das condições de saída de nosso algoritmo. Ainda nos resta mostrar que, quando o passo 8 for alcançado, a seqüência $g_1, ..., g_m$ é reduzida. Para tanto, é necessário demonstrar a validade do invariante entre colchetes no algoritmo. Antes disso, porém, estabeleceremos um lema técnico:

Lema 2.3.7. *Suponha que os invariantes entre colchetes sejam válidos no passo* 3. *Então,* $\|g_k\| \leq u$ *e grau* $g_{kj} < u$, $1 \leq j < i$ *no laço* 4.

Demonstração

Dado $k \in \{1, ..., m\}$, temos que ambas as desigualdades são válidas para $i = 1$. Se valerem ao término do passo i, $1 \leq i < k-1$, sejam $q, r \in R$, *grau* $r <$ *grau* g_{i+1i+1}, com $g_{ki+1} = qg_{i+1i+1} + r$ (I) e $g'_k = g_k - qg_{i+1}$ (II) . Observe que a divisão com resto está bem definida, pois, pela proposição anterior, $g_i \neq 0$ em qualquer momento do algoritmo e, como estamos supondo que $(g_1, ..., g_{k-1})$ é reduzida, *grau* $g_{i+1i+1} =$ *grau* $g_{i+1} \geq 0$.

De (II), segue que $\|g'_k\| \leq max\{\|g_k\|, \|qg_{i+1}\|\}$. Se $q = 0$, nada há a verificar. Caso contrário, $\|qg_{i+1}\| =$ *grau* qg_{i+1i+1} e, utilizando (I), vem $\|g'_k\| =$

$grau\ g_{ki+1} \leq \|g_k\|$. Logo, $\|g'_k\| \leq \|g_k\|$, que é limitado por u pela hipótese de indução.

Por outro lado, se $1 \leq j \leq i$, $grau\ g'_{kj} = grau(g_{kj} - qg_{i+1j}) \leq max\{grau\ g_{kj}, grau(qg_{i+1j})\}$. Mas $grau(qg_{i+1j}) < grau(qg_{i+1i+1}) \leq \|g_k\| \leq u$, utilizando inicialmente o fato de a seqüência ser reduzida e, em seguida, a igualdade (I). Além disso, se $1 \leq j < i$, $grau\ g_{kj} < u$ pela hipótese de indução. Portanto, resta mostrar que $grau\ g_{ki} < u$, que é conseqüência da passagem anterior pelo laço, quando a subtração em 5 aniquilou o termo líder de g_{ki}, que já sabíamos ser limitado por u pela hipótese de indução. □

Agora, estabeleceremos o resultado que desejávamos:

Proposição 2.3.8. *Sempre que o algoritmo passa pelo passo* 3*, a seqüência* $(g_1, ..., g_{k-1})$ *é reduzida e* $\|g_i\| \leq \|g_{i+1}\|$*, para* $1 \leq i < m$*. Em particular, o algoritmo retornará a resposta esperada se o passo* 8 *for alcançado.*

Demonstração

Os invariantes verificam-se trivialmente antes da primeira passagem pelo passo 2, e suponhamos que eles valham antes de uma determinada passagem por 3. O conjunto $g_1, ..., g_{k-1}$ não se modifica entre os passos 3 e 5, de forma que o primeiro invariante vale novamente no passo 3 se a condição em 6 for verdadeira. Caso contrário, ele será garantido pelo lema anterior e as ações tomadas no passo 7. Além disso, os g_i's são reordenados no passo 6 se a condição for verdadeira, de forma que o segundo invariante é novamente verificado depois do passo 6 e na próxima passagem pelo passo 3. Em particular, $(g_1, ..., g_m)$ é seqüência reduzida se o algoritmo atingir o passo 8. □

Temos ainda que provar que o passo 8 é de fato atingido, o que será conseqüência imediata da proposição a seguir.

Proposição 2.3.9.

(i) A propriedade $\|g_i\| < d$, $i = 1, 2, ..., m$ *vale durante todo o algoritmo.*

(ii) Definamos a função $s(g_1, ..., g_m) = \sum_{i=1}^{m} \|g_i\|$. *Essa função é não crescente no decorrer do algoritmo e decresce estritamente quando a condição no passo* 6 *vale. Como conseqüência, essa condição pode ser satisfeita no máximo* md *vezes e o número de vezes em que se faz o laço* 2 *é limitado por* $(m-1)(md+1)$.

Demonstração

(i) Por hipótese, o valor $max\{\|g_i\|, 1 \leq i \leq m\}$ é inferior a d no princípio. Além disso, alterações em $\|g_i\|$ só podem ocorrer nos passos 4 e 5, e isso quando $k = i$. Mas o lema (2.3.7) garante que, ao final do laço 4, a norma $\|g_k\|$ não excede u, que é justamente o valor anterior de $\|g_k\|$, logo permanece inferior a d.

(ii) Pelo mesmo motivo que em (i), o valor de s só poderá sofrer alteração nos passos 4 e 5. Mas o lema (2.3.7) assegura que o novo valor de $\|g_k\|$ não supera o antigo quando o laço for concluído. Conseqüentemente, s é não crescente. Além disso, é evidente que s terá decrescido se, e somente se, a condição do passo 6 houver sido satisfeita. Pelo item (i), sabemos que s é limitada por md no início do algoritmo e, baseados na proposição (2.3.6), garantimos que s é sempre um inteiro não negativo, pois nenhum g_i é nulo. Portanto, s não poderá decrescer mais do que md vezes. Mas entre duas ocasiões em que a condição do passo 6 é verdadeira, pode haver apenas $m-1$ em que ela é falsa, inclusive antes da primeira e depois da última. Então, o número de iterações do passo 2 se limita por $(m-1)(md+1)$. Em particular, o algoritmo termina. □

Reuniremos o que foi feito até agora no seguinte teorema, que também considerará a complexidade desse algoritmo:

Teorema 2.3.10. *O algoritmo (2.3.4) devolve o resultado esperado e requer* $O(nm^3dM(d))$ *operações aritméticas em* F.

Demonstração

A validade vem do que já foi feito. De fato, provamos inicialmente que o algoritmo retornaria a resposta correta se terminasse e, em seguida, que ele realmente termina. Com relação à complexidade, observamos que o passo de fato custoso computacionalmente é o passo 5, onde ocorrem operações aritméticas sobre R. A cada execução do passo 5, há $O(n)$ operações aritméticas em R, cada uma delas com um custo limitado por $O(M(d))$. A cada passagem pelo laço 2, o passo 5 poderá se repetir $O(m)$ vezes, o que nos dá $O(nmM(d))$ operações por passagem em 2. Mas, de acordo com a proposição anterior, há no máximo $(m-1)(md+1)$ dessas passagens, e o custo total será de $O(nm^3dM(d))$ operações aritméticas em F. □

Vimos nessa seção como uma seqüência reduzida associada a um reticulado sobre $F[y]$ pode ser obtida. Mencionamos na seção 2 que isso seria a ferramenta teórica para solucionar o problema da obtenção dos fatores irredutíveis em $F[x,y]$ de um polinômio de que conhecemos a fatoração módulo $m \in F[y]$. Isso será objeto da próxima seção.

2.4 Um algoritmo em tempo polinomial para fatorar polinômios em duas variáveis

O problema que nos propusemos a tratar no presente capítulo está próximo de uma solução. Partimos de uma idéia simples (2.1.1) e fomos pouco a pouco incorporando melhorias. Nesse momento, veremos como a teoria da seção

anterior nos fornece o ingrediente que faltava. O primeiro passo será relacionar fatores de f em $F[x,y]$ a fatores de f módulo m sujeitos a certas restrições.

Identificaremos um polinômio $f \in F[x,y] = (F[y])[x]$ de grau n na variável x com o seu vetor de coeficientes em $F[y]^{n+1}$ e consideraremos $\|f\|$ a norma do máximo associada a esse vetor. A seguinte proposição estabelece que se dois polinômios em $F[x,y]$ têm um divisor comum não constante módulo $m \in F[y]$, com m maior do que a sua resultante, então eles têm um divisor comum não constante em $F[x,y]$. Na demonstração, serão utilizadas propriedades de resultantes de dois polinômios que podem ser encontradas em livros elementares de Álgebra, como [Garcia e Lequain, 2002], por exemplo.

Proposição 2.4.1. *Sejam F um corpo, $f, g \in F[x,y] = R[x]$ com graus n, k em x, respectivamente, e $u \in R[x]$ polinômio mônico e não constante que divide tanto f quanto g módulo $m \in R$, onde $k\ grau_y f + n\ grau_y g < grau_y m$. Então, o polinômio $mdc(f,g) \in R[x]$ não é constante com respeito a x.*

Demonstração

Suponha, por absurdo, que $mdc(f,g) = 1$ em $F(y)[x]$. Então, existem $s, t \in R[x]$ tais que $sf + tg = Res_x(f,g)$, por propriedade de resultantes. Mas u divide f e g módulo m, logo divide $Res_x(f,g)\ mod\ m$. Outra propriedade das resultantes garante que $Res_x(f,g) \equiv 0\ mod\ m$, pois o $mdc(f,g)$ é divisível pelo polinômio mônico não constante u em $(F[y]/(m))[x]$. Mas $grau_y(Res_x(f,g)) \leq k\ grau_y f + n\ grau_y g < grau_y m$ implica $Res_x(f,g) = 0$, o que contradiz a hipótese de que $mdc(f,g) = 1$. Logo, $mdc(f,g) \in R[x]$ não é constante com respeito a x. □

A idéia do algoritmo de fatoração será a seguinte: sejam $f \in F[x,y]$ o polinômio que se deseja fatorar e u um fator mônico de f módulo $m \in F[y]$ de grau $k < n$. Procuraremos um polinômio "pequeno" $g \in F[x,y]$ tal que $n\|g\| < \frac{m}{k}\|f\|$. Se tal g for encontrado, obteremos uma fatoração não trivial de f em $F[x,y]$ pela proposição acima.

Para encontrar g com grau em x inferior a uma determinada cota j, consideraremos o reticulado $L \subseteq F[y]^j$ gerado pelos vetores de coeficientes de

$$\{ux^i; 0 \leq i < j-k\} \cup \{mx^i; 0 \leq i < k\}.$$

Um elemento de L pode ser escrito na forma $g = qu + rm$, com $q, r \in F[x,y]$, $grau_x q < j-k$ e $grau_x r < k$. Logo, $grau_x g < j$ e u divide g módulo m. Reciprocamente, se $g \in F[x,y]$ tem grau em x inferior a j e é divisível por u módulo m, então $g = q^*u + r^*m$ para certos $q^*, r^* \in F[x,y]$. Como u é mônico com respeito a x, podemos realizar divisão euclideana e obter $\bar{q}, \bar{r} \in F[x,y]$, $grau_x \bar{r} < k = grau_x u$, com $r^* = \bar{q}u + \bar{r}$. Definimos $q = q^* + m\bar{q}, r = \bar{r}$, de forma que $g = q^*u + r^*m = (q - m\bar{q})u + (\bar{q}u + \bar{r})m = qu + rm$. Note que $grau_x r < k = grau_x u$, e, conseqüentemente, $grau_x q \leq j-k$, isto é, $g \in L$. Provamos que

$$g \in L \Longleftrightarrow grau_x(g) < j \text{ e u divide } g \text{ módulo } m. \tag{2.1}$$

Portanto, poderemos utilizar redução de base para encontrar um vetor g em L "pequeno" com as propriedades desejadas.

Com isso, estamos prontos para enunciar um algoritmo em tempo polinomial para fatorar polinômios em $F[x,y]$. Os quatro primeiros passos são os mesmos do algoritmo que fatora polinômios livres de quadrados via levantamento de Hensel, mas há um sensível aumento no tamanho de l, o que exigirá mais iterações do passo de Hensel.

Algoritmo 2.4.2. *Algoritmo polinomial para fatoração em $F[x,y]$*

Entrada: *Um polinômio primitivo f em $R[x] = F[x,y]$, onde $R = F[y]$, onde F é um corpo com pelo menos $4nd$ elementos e fatoração efetiva para polinômios em uma variável. Aqui, $n = grau_x f \geq 1$, $d = grau_y f$, e $mdc(f, \frac{\partial f}{\partial x}) = 1$ em $F(y)[x]$.*

Saída: *Os fatores irredutíveis $\{f_1, ..., f_k\} \subseteq F[x,y]$ de f.*

1. *se $n = 1$ então devolva f*

$b \leftarrow cl_x(f)$

escolha $U \subseteq F$ *de cardinalidade* $\sharp U = 4nd$

2. *repita*

   escolha aleatoriamente $v \in U,\ \bar{f} \leftarrow f(x, v)$

   até que $b(v) \neq 0$ *e* $mdc(\bar{f}, \frac{\partial \bar{f}}{\partial x}) = 1$ *em* $F[x]$.

   $l \leftarrow 2nd$

3. {*Fatoração modular*}

   utilize um algoritmo de fatoração em uma variável para calcular $f \equiv bh_1...h_r \ mod\ (y - v)$ *em* $(F[y]/(y - v))[x] \simeq F[x]$, *para certos polinômios mônicos irredutíveis* $h_1, ..., h_r$ *em* $F[x]$.

4. {*Levantamento de Hensel*}

   $a \leftarrow b(v)^{-1}$

   utilize o Algoritmo de Euclides Estendido para calcular uma árvore de fatoração de f *módulo* $y - v$ *em* $F[x]$ *com folhas* $h_1, ..., h_r$.

   utilize o Levantamento de Hensel de Múltiplos Fatores para calcular uma fatoração $f \equiv bg_1...g_r \ mod\ (y - v)^l$, *para polinômios* $g_1, ...g_r$ *em* $F[x, y]$ *que são mônicos com respeito a* x *e tais que* $grau_y g_i < l$ *e* $g_i(x, v) = h_i$, $1 \leq i \leq r$.

5. {*Inicialização do conjunto de índices* T *de fatores modulares ainda não considerados, do conjunto* G *de fatores encontrados, e do polinômio* $f^\star$ *a ser fatorado*}

   $T \leftarrow \{1, 2, ..., r\},\ \ s \leftarrow 1,\ \ G \leftarrow \emptyset,\ \ f^\star \leftarrow f$

6. {*Combinação de fatores*}

   enquanto $T \neq \emptyset$

7. *escolha* u *entre* $\{g_t; t \in T\}$ *de grau máximo em* x

   $k \leftarrow grau_x u, n^\star \leftarrow grau_x f^\star$

   {*Encontra o fator irredutível de* $f^\star$ *que é divisível por* $u \ mod\ p$}

   para $k < j \leq n^\star$ *faça*

8. {*Cálculo de vetor "pequeno"*}

   utilize o algoritmo (2.3.4) para obter um vetor pequeno $g^\star$ *no reticulado* $L \subseteq F[y]^j$ *gerado pelos vetores de coeficientes de*

   $$\{ux^i; 0 \leq i < j - k\} \cup \{p^l x^i; 0 \leq i < k\}$$

e também denote o polinômio correspondente por $g^\star$.

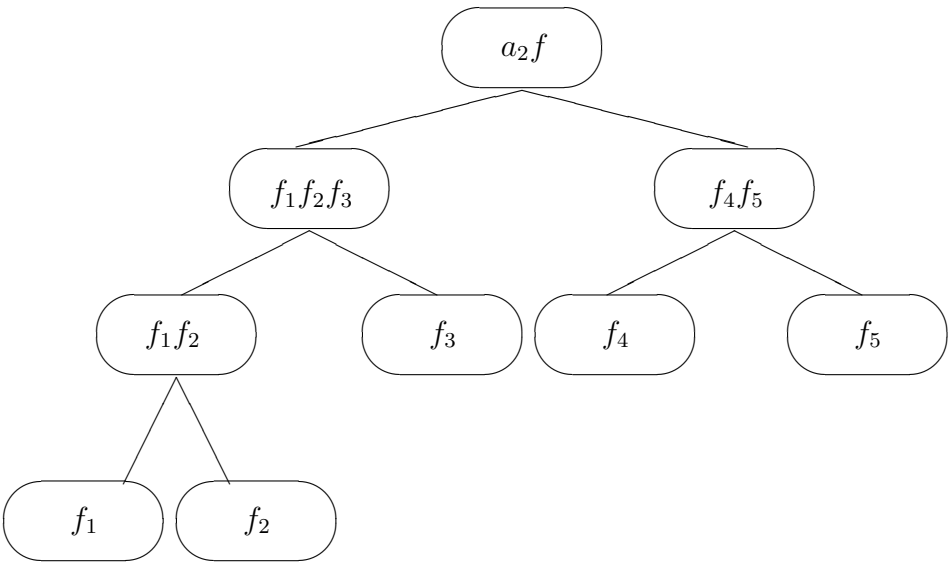
9. *determine por tentativas o conjunto* $S \subseteq T$ *de índices* i *para os quais* h_i *divide* $g^\star$ *módulo* $y - v$.
   calcule $h^\star \equiv b \prod_{i \in T \setminus S} g_i \ mod \ (y-v)^l$
   se $grau_y(f^\star) = grau_y(pp_x(g^\star)pp_x(h^\star))$ *então*
   $T \leftarrow T \setminus S, \ \ G \leftarrow G \cup \{pp_x(g^\star)\}, \ \ f^\star \leftarrow pp_x(h^\star)$
   interrompa o laço 7 *e vá para* 6

10. $T \leftarrow \emptyset$, $G \leftarrow G \cup \{f^\star\}$

11. *devolva* G

Apliquemos esse algoritmo ao exemplo 2.2.15:

Exemplo 2.4.3. *Lembremos que as condições não eram imediatamente satisfeitas, e portanto utilizamos uma adaptação com* $p = y^4 + y + 1$. *Retomemos então do ponto em que estávamos antes da recuperação dos fatores. Tínhamos a árvore de fatoração módulo* $(y^4 + y + 1)^{2^2}$ *dada por*



$a_2 = y^{12} + 1$

$$f_1 f_2 f_3 = x^3 + (y^{15} + y^7 + y + 1)x^2 + (y^{15} + y^{10} + y^8 + y^7 + y^4 + y^2 + 1)x + y^{11} + y^{10} + y^3 + y^2$$
$$f_1 f_2 = x^2 + (y^{15} + y^7 + y^3 + y + 1)x + y^{15} + y^8 + y^7 + y^3 + 1$$
$$f_4 f_5 = x^2 + (y^{15} + y^7)x + y^{10} + y^6$$
$$f_1 = x + y^{15} + y^7 + y^3$$
$$f_2 = x + y + 1$$
$$f_3 = x + y^3$$
$$f_4 = x + y^{15}$$
$$f_5 = x + y^7$$

Mas, conforme se comentou antes da apresentação do algoritmo, agora teremos que fazer mais levantamentos. De fato, para obtermos congruências módulo um polinômio de grau $2nd = 50$*, serão necessários* $\lceil log\ \frac{50}{4} \rceil = 4$ *levantamentos. Calculamos então os dois levantamentos ainda necessários para a obtenção da árvore de fatoração módulo* $(y^4 + y + 1)^{2^4}$ *e as entradas obtidas foram*

$$a_4 = y^{60} + y^{12}$$
$$f_1 f_2 f_3 = x^3 + (y^{63} + y^{31} + y + 1)x^2 + (y^{63} + y^{46} + y^{32} + y^{31} + y^{30} + y^{16} + 1)x + y^{47} + y^{46} + y^{41} + y^{30}$$
$$f_1 f_2 = x^2 + (y^{31} + y + 1)x + y^{32} + y^{31}$$
$$f_4 f_5 = x^2 + (y^{63} + y^{31})x + y^{46} + y^{14}$$
$$f_1 = x + y^{31}$$
$$f_2 = x + y + 1$$
$$f_3 = x + y^{63}$$
$$f_4 = x + y^{15}$$
$$f_5 = x + y^{63} + y^{31} + y^{15}$$

Agora, devemos recuperar os verdadeiros fatores a partir da fatoração $f \equiv y^4 f_1 f_2 f_3 f_4 f_5\ mod\ p^{16}$ *via redução de base. No passo* 7*, escolhemos um polinômio*

de grau máximo em x, digamos $f_1 = x + y^{31}$. Logo, $k = grau_x(f_1) = 1$ e, para $k = 1 < j \leq 5$, procuramos o verdadeiro fator de f em $F_2[x, y]$ divisível por f_1 módulo p^{16}. Quando $j = 2$, temos o reticulado L gerado pelos vetores $ux^0 = (1, y^{31}), p^l x^0 = (0, y^{64} + y^{16} + 1)$ em $F_2[y]^2$. Aplicando o algoritmo (2.3.4) para redução de base, obtemos a base $(1, y^{31}), (y^{33}, y^{16} + 1)$ para L, onde o vetor $(1, y^{31})$, associado ao polinômio $g^\star = x + y^{31}$ é minimal. É claro que apenas o índice 1 será incluído em S, pois $g^\star = g_1$. Portanto, $pp_x(h^\star) = pp_x(y^4 f_2 f_3 f_4 f_5) = y^3x^4 + (y^{34} + y^4 + y^3)x^3 + (y^{35}+y^{34}+y^{17}+y)x^2+(y^{48}+y^{32}+y^{18}+y^{17}+y^2+y+1)x+y^{49}+y^{48}+y^{33}+y^{32}+y+1$ e é claro que $5 = grau_y(f^\star) < 80 = grau_y(pp_x(g^\star)pp_x(h^\star))$. Aqui, vale uma observação: como $grau_y(pp_x(g^\star)) = 31 > 5$, o teste certamente falharia. Vemos portanto que podemos alterar o algoritmo de tal forma que $f^\star$ nem é calculado quendo o grau de $g^\star$ já é grande demais. Sigamos então para $j = 3$. O reticulado L é agora gerado pelos vetores $(1, y^{31}, 0), (0, 1, y^{31}), (0, 0, y^{64}+y^{16}+1)$ e, aplicando o algoritmo para redução de base, vem $g^\star = y^2x^2+y^{16}+1$. Novamente, o grau em y é excessivamente grande e não recuperaremos um fator de f em $F[x, y]$, o mesmo que ocorre para $j = 4$, quando obtemos $g^\star = x^3+y^{15}x^2+y^{14}x+y^{13}$. Para $j = 5$, porém, o reticulado L é gerado por $(1, y^{31}, 0, 0, 0), (0, 1, y^{31}, 0, 0), (0, 0, 1, y^{31}, 0), (0, 0, 0, 1, y^{31}), (0, 0, 0, 0, y^{64} + y^{16} + 1)$ e implica $g^\star = y^4x^4 + yx + 1$. Assim, $S = \{1, 3, 4, 5\}$ e $pp_x(h^\star) = pp_x(y^4(x + y + 1)) = x + y + 1$, o que faz com que o teste tenha resposta positiva e tenhamos encontrado o fator $g^\star = y^4x^4+yx+1$ de f em $F[x, y]$. Logo, $f^\star = x+y+1$ e $T = \{f_2\} = \{x+y+1\}$. Nesse caso, escolhemos o polinômio de grau máximo (e único) f_2 e definimos $k = 1$, $n^\star = 1$. O laço do passo 8 deveria ser feito para $1 = k < j \leq n^\star = 1$, logo não será realizado. Chegamos ao passo 9, onde G e T se tornam $\{y^4x^4 + yx + 1, x + y + 1\}$ e $\emptyset$, respectivamente. O algoritmo devolve G e obtemos a fatoração

$$f = (y^4x^4 + yx + 1)(x + y + 1)$$

em $F_2[x, y]$.

Resta-nos demonstrar a validade desse algoritmo, além de apresentar uma análise de sua complexidade computacional.

Teorema 2.4.4. *O algoritmo anterior obtém corretamente a fatoração de um polinômio nas condições prescritas. Um custo computacional de* $O(n^6 dM(nd))$ *operações aritméticas no corpo* F *ocorre no pior caso.*

Demonstração

Comecemos pela corretude desse algoritmo. Para prová-la, procederemos de maneira parecida ao que foi feito no teorema (2.1.3), demonstrando que os invariantes

(i) $f^\star \equiv b \prod_{i \in T} g_i \ mod \ (y-v)^l$

(ii) $b = cl_x(f^\star)$

(iii) $f = a f^\star \prod_{g \in G} g$, para algum $a \in F$

(iv) G é constituído apenas de elementos irredutíveis

são válidos a cada passagem pelo passo 6 do algoritmo.

Na primeira passagem por 6, temos $f^\star = f$, $b = cl_x(f)$ e $G = \emptyset$, logo todas as afirmações acima valem. Suponha que as afirmações anteriores sejam verdadeiras após uma determinada passagem por 6.

Se $T = \emptyset$, nada há a ser feito. Para $T \neq \emptyset$, consideremos $u \in \{g_t; t \in T\}$ de grau máximo. Afirmamos que g, o fator irredutível de $f^\star$ que é divisível por u módulo $(y-v)$, está associado a um vetor minimal do reticulado L gerado pelos coeficientes (em relação à variável x) de $\{ux^i; 0 \leq i < j-k\} \cup \{p^l x^i; 0 \leq i < k\}$ em $F[y]^j$, onde $j = grau_x(g)+1$. O fato de g estar em L vem do seguinte: pela escolha de v, segue que $cl_x(f)$ não é nulo $mod \ (y-v)$ e $f \ mod \ (y-v)$ é livre de quadrados. Além disso, u divide g módulo $(y-v)$, por construção, e u divide f módulo $(y-v)^l$ pela invariância (i), que supomos válida por hipótese de indução. Mas essas são as hipóteses para o corolário (2.2.8), logo u divide g módulo $(y-v)^l$. Além disso, $grau_x(g) < j$, o que implica $g \in L$ por (2.1). Se houvesse um polinômio $\tilde{g}$ em L de

norma inferior a g, teríamos que u também divide $\tilde{g}$ módulo $(y-v)$, pela equação (2.1), o que contradiria a irredutibilidade de g. Isso demonstra nossa afirmação.

O último argumento acima pode ser estendido. Se $\tilde{g} \in F[x,y]$ é um divisor de f divisível por u módulo $(y-v)$, então g divide $\tilde{g}$ em $F[x,y]$. Para tanto, basta observar que, como $f \ mod \ (y-v)$ é livre de quadrados, então g e $\tilde{g}$ têm um fator módulo p originado de um mesmo fator de f em $F[x,y]$. Conseqüentemente, $mdc(g,\tilde{g})$ não é constante em $F[x,y]$ e, pela irredutibilidade de g, $mdc(g,\tilde{g}) = g$ (a menos de constante), o que estabelece o resultado.

Seja $g^\star$ o polinômio associado ao vetor pequeno calculado no passo 8. Vejamos que a condição em 9 é satisfeita se, e somente se, $pp_x(g^\star h^\star) = cf^\star$, para algum $c \in F$. A necessidade é imediata. Reciprocamente, $pp_x(g^\star h^\star) = pp_x(bq\prod_{i\in T} g_i) \equiv pp_x(q)f^\star \ mod \ (y-v)^l$, para algum $q \in F[x,y]$. A condição em 9 garante que ambos os termos da congruência coincidem e que $pp_x(q)$ não depende de y, logo $pp_x(q)$ é uma constante c e $pp_x(g^\star h^\star) = cf^\star$.

Como $grau_x(g^\star) < j$ a cada passagem por 8, concluímos que a condição 9 será falsa sempre que $j \leq grau_x(g)$. Em particular, se $f^\star$ é irredutível e $\sharp T = 1$, esse teste sempre terá resposta negativa e por isso o passo 10 e a hipótese de indução garantem que as afirmações (i), (ii), (iii) e (iv) estão corretas ao fim do laço 6.

Suponhamos então que $grau_x(g) < n^\star$ e seja $j = 1+grau_x(g)$. Mostremos que o teste do passo 9 terá resposta positiva:

$$grau_x(g^\star)\, grau_y(g)+grau_x(g)\, grau_y(g^\star) = (j-1)grau_y g+(j-1)grau_y g^\star < nd+nd = 2nd,$$

pois g é um fator de $f^\star$, e $grau_y(g^\star) = grau_y(g)$, já que g também gera um vetor minimal em L. Como $2nd = grau_y(y-v)^l$, aplicamos a proposição (2.4.1) para determinar que $mdc(g,g^\star)$ não é uma constante em $F[x,y]$ e, visto que g é irredutível e $g^\star$ é mínimo, $g = k\ pp_x(g^\star)$, para alguma constante $k \in F$.

Sejam $h = f^\star/g$ e $S \subseteq T$ como no passo 9 do algoritmo. Mostraremos que $h = pp_x(h^\star)$ utilizando a unicidade de levantamento de Hensel (teorema (2.2.7)).

Para tanto, verificaremos as hipóteses desse teorema para $cl_x(g)h$ e $cl_x(h)g$, que discriminamos como $(a), (b), (c)$ no que vem a seguir .

Consideraremos $cl_x(g)h$, $cl_x(h)g$, $h^\star$ e $\bar{g} \equiv b\prod_{i\in S} g_i \ mod\ (y-v)^l$ em $F[x,y]$, com grau em y inferior a l. Como f é livre de quadrados módulo $(y-v)$, vale que $cl_x(g)h$ e $cl_x(h)g$ são relativamente primos módulo $(y-v)$. Além disso, seus coeficientes líder não dividem zero módulo $(y-v)$, pois isso não ocorre com o coeficiente líder de $f^\star$.

(a) $\bar{g} \equiv b\prod_{i\in S} g_i \equiv cl_x(h)cl_x(g)\prod_{i\in S} g_i \equiv cl_x(h)g \ mod\ (y-v)$.
$grau_x(cl_x(h)g) = grau_x(g) = grau_x(pp_x(g)) = grau_x(g^\star) = grau_x(\bar{g})$
$cl_x(\bar{g}) = b = cl_x(f^\star) = cl_x(gh) = cl_x(cl_x(h)g)$

(b) $cl_x(g)h = cl_x(g)f^\star/g \equiv cl_x(g)b\prod_{i\in T} h_i/g \equiv b\prod_{i\in T\setminus S} h_i \equiv h^\star \ mod\ (y-v)$
$grau_x(h^\star) = grau_x(f^\star/g^\star) = grau_x(f^\star) - grau_x(g) = grau_x(h) = grau_x(cl_x(g)h)$
O coeficiente líder $lc_x(g)h = lc_x(g)f^\star/g$ *é* naturalmente $b = lc_x(f^\star)$, que *é*,
por construção, o coeficiente líder de $h^\star$

(c) $cl_x(g)h\ cl_x(h)g = cl_x(gh)gh = bf^\star \equiv \bar{g}h^\star \ mod\ (y-v)^l$,
pois $b = cl_x(f^\star)$ e $f^\star \equiv b\prod_{i\in T} g_i \ mod\ (y-v)^l$.

Utilizando a unicidade do levantamento de Hensel (teorema (2.2.7)), segue que $lc(g)h \equiv h^\star \ mod\ (y-v)^l$, logo coincidem pois têm grau na variável y inferior a l. Conseqüentemente, $h = pp_x(h^\star)$ e $f^\star = gh = k\ pp_x(g^\star)pp_x(h^\star)$, o que implica que $g^\star, h^\star$ satisfazem a condição do passo 9.

Portanto, se $f^{\star\prime}$, b' e G' denotam os valores atualizados de $f^\star$, b e G, respectivamente, vem que:

(i) $f^{\star\prime} = pp_x(h^\star) = cl_x(h^\star)\prod_{i\in T\setminus S} g_i = b'\prod_{i\in T'} g_i \ mod\ (y-v)^l$

(ii) $b' = cl_x(pp_x(h^\star) = cl_x(f^{\star\prime})$

(iii) $f = af^\star\prod_{g\in G} g = akpp_x(g^\star)pp_x(h^\star)\prod_{g\in G} g = akf^{\star\prime}\prod_{g\in G'} g$

(iv) $G' = G \cup \{pp_x(g^\star)\}$, logo é constituído apenas de elementos irredutíveis porque $pp_x(g^\star) = k^{-1}g$ e g é irredutível.

Isso implica imediatamente que o algoritmo retorna um conjunto G contendo todos os fatores irredutíveis de f. Apenas o termo líder de f precisa ser recomposto.

Analisemos então seu tempo de computação: conforme visto na análise do algoritmo (2.2.12), o tempo de computação envolvido nos cinco primeiros passos é de $O(nd + M(n)log\ n)$ para o passo 2, $O(M(n^2)log\ n + M(n)log(n)log(q))$ para o passo 3, se $F = F_q$, e $O(M(n)log(n)M(nd))$ para o passo 4 (a alteração no passo 4 se deve ao aumento na cota l). Mas essa análise ficará em segundo plano, pois o custo do algoritmo será dominado pelo custo de cálculo do vetor pequeno no passo 8. Inicialmente, note que temos que a norma de cada um dos j geradores do reticulado é limitada por $2nd$, o grau em y de $(y-v)^l$. Mas, pelo teorema (2.3.10), o tempo de computação em cada passo é de $O(j^4ndM(nd))$. Sejam $f_1, ..., f_r \in F[x,y]$ os fatores irredutíveis de f. Pelo que provamos na demonstração de validade do teorema, o passo 7 é repetido para $j = 2, ..., 1 + grau_x f_i$ (sendo o limite à esquerda 2 uma cota no pior caso). Assim, o custo total das passagens pelos passos 7 e 8 é limitada por

$$\begin{aligned} &\sum_{i=1}^{r} \sum_{j=1}^{grau_x(f_i)+1} j^4 ndM(nd) \\ &\quad \leq ndM(nd) \sum_{i=1}^{r} (1 + grau_x(f_i))^5 \\ &\quad \leq ndM(nd) r (\frac{r+n}{r})^5 \end{aligned} \tag{2.2}$$

A primeira majorização se deve ao fato de que $\sum_{j=2}^{N} j^4 = \frac{1}{5}(N+1)^5 - \frac{1}{2}(N+1)^4 + \frac{1}{3}(N+1)^3 - \frac{1}{30}N - \frac{31}{30}$ e a segunda, do fato que o ponto de máximo absoluto da função $\Phi(x_1, ..., x_n) = \sum_{i=1}^{n} x_i^5$ sobre o hiperplano $\sum_{i=1}^{n} x_i = r > 0$ em $\mathbb{R}^n$, com $x_i \geq 0, \forall i$, é $(x_1, ..., x_n) = (\frac{r}{n}, ..., \frac{r}{n})$. Logo, o número de operações aritméticas sobre F nesse trecho do algoritmo tem $O(n^6 dM(nd))$.

O restante do algoritmo não tem passos custosos computacionalmente. Logo, o custo total se deriva do laço dos passos 6, 7 e 8 e tem $O(n^6 dM(nd))$. □

Encontramos portanto um algoritmo em tempo polinomial para resolver o problema de fatoração de polinômios em duas variáveis sobre corpos que admitem fatoração efetiva de polinômios em uma variável. Como já foi mencionado anteriormente, esse algoritmo nada mais é do que uma redução em tempo polinomial do caso bivariado ao univariado, pois a fatoração é de fato calculada em $(F[y]/(y-v))[x] \approx F[x]$. A adaptação desse algoritmo a corpos com menos de $4nd$ elementos é feita do mesmo modo como explicamos na observação após o algoritmo (2.2.12). O custo dessa adaptação claramente permanece polinomial.

3 FATORANDO POLINÔMIOS VIA UMA EQUAÇÃO DIFERENCIAL

No capítulo anterior, obtivemos um algoritmo em tempo polinomial para determinar os fatores irredutíveis de um polinômio em duas variáveis sobre um corpo F. O presente capítulo apresentará, de forma generalizada, um segundo algoritmo para esse problema, proposto por S. Gao em [Gao, 2003]. Uma de suas vantagens é a recuperação simultânea dos fatores irredutíveis racionais e absolutos de um dado polinômio em duas variáveis.

3.1 Uma extensão do Algoritmo de Gao

Sejam F um corpo e $\bar{F}$ o seu fecho algébrico. Dado um polinômio $f \in F[x, y]$, desejamos encontrar seus fatores irredutíveis sobre F e sobre $\bar{F}$. Um fator irredutível de f sobre F é denominado *fator irredutível racional*. Sobre $\bar{F}$, é dito *fator absolutamente irredutível*. Calculando $f/mdc(f, \frac{\partial f}{\partial x})$, podemos reduzir f ao caso em que $mdc(f, \frac{\partial f}{\partial x}) = 1$.

Dado um polinômio $g \in \bar{F}[x, y]$, identificamo-lo com seus associados αg, onde $\alpha \in \bar{F}$ e $\alpha \neq 0$. Em particular, podemos supor que g possui pelo menos um termo com coeficiente unitário, de forma que seus coeficientes estão contidos em uma extensão de grau mínimo.

Já que estamos supondo $mdc(f, \frac{\partial f}{\partial x}) = 1$ em $F[x, y]$, f é livre de quadrados e cada um de seus fatores tem grau maior ou igual a um na variável x. Seja a fatoração $f = f_1 ... f_r$, onde $f_i \in \bar{F}[x, y]$ são distintos e irredutíveis sobre $\bar{F}$, isto é, absolutamente irredutíveis.

No estudo da fatoração de polinômios em uma variável sobre corpos finitos, a incorporação de métodos da Álgebra Linear surgiu com o trabalho de Berlekamp [Berlekamp, 1970]. Um outro método para fatoração de polinômios em

$F_{p^n}[x] = GF(p^n)[x]$ baseado na Álgebra Linear foi desenvolvido por Niederreiter [Niederreiter, 1993], que utilizou as soluções polinomiais de uma equação diferencial, obteníveis pela resolução de um sistema linear, para decompor o polinômio f em fatores menores. Gao [Gao, 2003] desenvolveu uma teoria similar para polinômios em duas variáveis, modificando ligeiramente um problema diferencial inicialmente enunciado por Ruppert [Ruppert, 1999]. Ruppert estava mais interessado em desenvolver um teste para determinar a irredutibilidade absoluta de polinômios e considerou equação diferencial parcial

$$\frac{\partial}{\partial y}(\frac{g}{f}) = \frac{\partial}{\partial x}(\frac{h}{f}), \tag{3.1}$$

onde $g, h \in \bar{F}[x, y]$. De fato, essa equação vem da Análise e fornece uma condição para que a 1-forma diferencial $\frac{g}{f}dx + \frac{h}{f}dy$ seja fechada. Além disso, e essa foi uma importante contribuição de Gao, limitaram-se os graus dos polinômios g e h no espaço solução a $grau\ g \leq (m-1, n)$, $grau\ h \leq (m, n-1)$, onde (m, n) denota o grau de f em x e y, respectivamente. A título de curiosidade, Ruppert restringia o grau de h a $grau\ h \leq (m, n-2)$.

A equação diferencial acima, em conjunto com as restrições nos graus de g e h determinadas por Gao, integrará o que denominaremos de *Problema de Gao associado a* f. Diremos simplesmente que g satisfaz o problema de Gao associado a f se existir um polinômio h com a propriedade de que (g, h) é uma solução do problema de Gao associado a f.

Observe que a equação (3.1) pode ser reescrita na forma

$$f(\frac{\partial g}{\partial y} - \frac{\partial h}{\partial x}) + h\frac{\partial f}{\partial x} - g\frac{\partial f}{\partial y} = 0. \tag{3.2}$$

Como a diferenciação é linear sobre $\bar{F}$, essa equação origina um sistema de equações lineares nos coeficientes de g e h. Portanto, todas as soluções g, h formam um espaço vetorial sobre $\bar{F}$ e, pelo mesmo motivo, sobre F. Devido ao fato de que $mdc(f, \frac{\partial f}{\partial x}) = 1$, não é difícil estabelecer que, para cada $g \in \bar{F}[x, y]$, existe no

máximo um $h \in \bar{F}[x,y]$ satisfazendo o problema de Gao. Definamos

$$\begin{aligned} \bar{G} &= \{g \in \bar{F}[x,y]; g \text{ satisfaz o problema de Gao}\} \\ G &= \{g \in F[x,y]; g \text{ satisfaz o problema de Gao}\} \end{aligned} \tag{3.3}$$

Então $G \subset \bar{G}$. Por cálculos simples, verificamos que $g = \frac{\partial f}{\partial x}$ e $h = \frac{\partial f}{\partial y}$ satisfazem o problema de Gao, de forma que $\frac{\partial f}{\partial x} \in G \subset \bar{G}$. Também é imediato verificar que G e $\bar{G}$ têm dimensão finita sobre F e $\bar{F}$, respectivamente. O seguinte teorema caracteriza um subespaço vetorial de G de grande importância. Esse resultado e suas conseqüências são tratados aqui com maior generalidade do que em Gao [Gao, 2003], pois não se incluirá nenhuma restrição na característica do corpo sobre o qual o polinômio está definido. Observamos que Gao exigia que a característica do corpo fosse nula ou superior a $(2m-1)n$, onde m e n são os graus do polinômio f nas variáveis x e y, respectivamente.

Teorema 3.1.1. *Sejam F um corpo e $f \in F[x,y]$, onde $mdc(f, \frac{\partial f}{\partial x}) = 1$ e grau $f = (m,n)$. Suponha que f tenha r fatores irredutíveis distintos em $\bar{F}[x,y]$, $f = f_1 ... f_r$.*

Então, existe um subespaço vetorial G' de G de dimensão r tal que, se $g \in G'$, g pode ser escrito na forma $g = \sum_{i=1}^{r} \lambda_i E_i$, com $E_i = \frac{f}{f_i}\frac{\partial f_i}{\partial x}$, $\lambda_i \in \bar{F}$, $1 \leq i \leq r$.

Demonstração

A demonstração desse teorema utiliza as idéias de um teorema análogo de Gao [Gao, 2003].

É fácil ver que os elementos E_i assim definidos satisfazem

$$\frac{\partial f}{\partial x} = E_1 + E_2 + ... + E_r, \;\; E_i E_j \equiv 0 \; mod \; f, \;\; \forall i \neq j. \tag{3.4}$$

Usando esse fato, segue que $E_i \in \bar{F}[x,y]$ e E_i satisfaz o problema de Gao, $\forall i$. Seja então o subespaço $\bar{G}'$ de $\bar{G}$ gerado por esses elementos. Vejamos que esse espaço tem dimensão r provando a independência linear dos E_i's: sejam $a_1, a_2, ..., a_r \in \bar{F}$ tais que $a_1E_1 + a_2E_2 + ... + a_rE_r = 0$. Seja $i \in \{1, 2, ..., r\}$. Note que $a_iE_i = -\sum_{j \neq i} a_jE_j$

implica que f_i divide E_j, $\forall i \neq j$. Logo, f_i divide $a_i E_i$. Mas $mdc(f_i, \frac{f}{f_i}\frac{\partial f_i}{\partial x}) = 1$, pois $mdc(f_i, \frac{f}{f_i}) = 1 = mdc(f_i, \frac{\partial f_i}{\partial x})$. Portanto, $a_i = 0$.

Construiremos agora um subconjunto $\{g_1, g_2, ..., g_r\}$ de elementos linearmente independentes em G tal que $< g_1, g_2, ..., g_r >_{\bar{F}} = < E_1, E_2, ..., E_r >_{\bar{F}}$, utilizando elementos algebricamente conjugados aos E_i's. Quando esse resultado for estabelecido, teremos um subespaço vetorial G' de G satisfazendo a condição requerida no enunciado do teorema.

Se todos os E_i's estão em G, nada há a ser feito. Suponha que algum E_i, digamos E_1, não está em G. A relação entre os fatores absolutamente irredutíveis de f e as extensões algébricas de F será melhor explicitada em dois fatos que serão enunciados e demonstrados abaixo.

Fato 1: Para todo automorfismo σ de $\bar{F}$ que coincide com a identidade em F, $\sigma(f_1)$ também é um fator absolutamente irredutível de f e $\sigma(E_1)$ corresponde naturalmente a $\sigma(f_1)$.

Observe que $f = \sigma(f) = \sigma(f_1 f_2 ... f_r) = \sigma(f_1)\sigma(f_2)...\sigma(f_r)$. Logo, decompusemos f em r fatores não triviais, conseqüentemente, em r fatores absolutamente irredutíveis.

Além disso, $\sigma(E_1) = \sigma(\frac{f}{f_1}\frac{\partial f_1}{\partial x}) = \frac{\sigma(f)}{\sigma(f_1)}\sigma(\frac{\partial f_1}{\partial x}) = \frac{f}{\sigma(f_1)}\frac{\partial \sigma f_1}{\partial x}$, o que estabelece uma correspondência natural entre $\sigma(f_1)$ e $\sigma(E_1)$. Quando dois fatores de f forem relacionados dessa forma, isto é, quando existir um automorfismo em $\bar{F}$ que restrito a F é a identidade associando esses fatores, diremos que eles são algebricamente conjugados. Essa nomenclatura estende a definição usual de elementos algebricamente conjugados em extensões de corpos.

Fato 2: Os coeficientes de E_1 e f_1, vistos como polinômios em $\bar{F}[x, y]$, determinam a mesma extensão de F. Seja K essa extensão de F. Então, K é separável sobre F com dimensão $[K : F] = l$, onde l é o número de elementos distintos algebricamente conjugados a f_1.

Sejam K_1 e K_2 as extensões pelos coeficientes de E_1 e f_1, respectivamente. Os coeficientes de E_1 são os coeficientes de $\frac{f}{f_1}\frac{\partial f_1}{\partial x}$. Mas os coeficientes de $\frac{f}{f_1}$ determinam a mesma extensão dos de f_1, e como os coeficientes de $\frac{\partial f_1}{\partial x}$ estão na extensão definida pelos coeficientes de f_1, vale que $K_1 \subseteq K_2$. A recíproca também pode ser verificada sem maiores dificuldades e $K = K_1 = K_2$ está bem definido.

O corpo K é uma extensão algébrica finitamente gerada. Portanto, existe um polinômio mônico irredutível $h \in F[t]$, o polinômio minimal, tal que $K \approx F[t]/(h)$.

Vejamos inicialmente que o número de homomorfismos distintos de K em $\bar{F}$ que restritos a F são a identidade é igual a l. Por um lado, existem pelo menos l desses homomorfismos, pois, para cada fator absolutamente conjugado de f_1, há um automorfismo de $\bar{F}$ que é a identidade quando restrito a F e leva f_1 a esse fator. Logo, se os fatores são distintos, esses automorfismos agem de forma distinta sobre f_1, e sua restrição a K também é distinta. Por outro lado, se $\psi_1, ..., \psi_l$ são os homomorfismos de K em $\bar{F}$ criados dessa maneira e ψ é um homomorfismo de K em $\bar{F}$ que coincide com a identidade em F, existe uma extensão $\bar{\psi} : \bar{F} \to \bar{F}$ de ψ, pois $\bar{F}$ é algébrico sobre K. Pelo *fato* 1, $\bar{\psi}$ leva f_1 a algum de seus fatores absolutamente conjugados, isto é, coincide com algum ψ_j sobre os coeficientes de f_1. Mas esses coeficientes determinam K, logo $\psi = \psi_j$. A separabilidade vem do fato de que os fatores absolutamente irredutíveis de f são todos distintos, concluindo a demonstração do fato 2.

Então, existem l imersões distintas $\sigma_1, \sigma_2, ..., \sigma_l$ de K em $\bar{F}$ fixando F que geram os l elementos algebricamente conjugados $\sigma_1 E_1, \sigma_2 E_1, ..., \sigma_l E_1$ de E_1 sobre F. Da Teoria de Corpos, sabemos que existe $\alpha \in K$ tal que $K = F(\alpha)$ e $1, \alpha, ..., \alpha^{l-1}$ formam uma base de K sobre F.

Para $1 \leq i \leq l$, definamos $e_i = \sum_{j=1}^{l} \sigma_j(\alpha^i E_1) = \sum_{j=1}^{l} \sigma_j(\alpha^i)\sigma_j E_1$. Então, $e_i \in F[x, y]$, $e_i \in G$ e $< e_1, ..., e_l >_{\bar{F}} = < E_1, ..., E_l >_{\bar{F}}$.

Demonstremos as afirmações acima: o fato de e_i estar em G é verificável por um cálculo simples. Como e_i nada mais é que a aplicação do operador traço a $\alpha^i E_1$, esse polinômio terá seus coeficientes em F. Finalmente, vemos que $\sigma_j E_1 = E_k$, para certo k em $\{1, 2, ..., r\}$. Logo, $e_i \in < E_1, ..., E_r >_{\bar{F}}$, $\forall i$. Além disso, um teorema conhecido da Teoria de Corpos garante que a matriz de automorfismos de ordem l dada por $(\sigma_j(\alpha^i))_{0 \leq i \leq l-1, 1 \leq j \leq l}$ é não singular. Como $\sigma_1 E_1, ..., \sigma_l E_1$ são linearmente independentes sobre $\bar{F}$, os polinômios $e_1, ..., e_l$ também o são.

Aplicando esse processo aos elementos $E_i \notin G \cup \{\sigma_1 E_1, ..., \sigma_l E_1\}$, obteremos r elementos $e_1, ..., e_r \in G$ linearmente independentes sobre $\bar{F}$ e, em particular, sobre F, satisfazendo as condições do teorema. □

Uma conseqüência imediata desse teorema é:

Corolário 3.1.2. *Se $dim_F G = 1$, então f é absolutamente irredutível.*

Exemplo 3.1.3. *Aplicaremos esse resultado ao polinômio $f(x, y) = x^2 + y + 1$ em $\mathbb{Q}[x, y]$. Para tanto, será necessário encontrar as soluções polinomiais g e h para a equação $\frac{\partial}{\partial y}(\frac{g}{f}) = \frac{\partial}{\partial x}(\frac{h}{f})$, sendo os graus de g e h nas variáveis (x, y) limitados por $(1, 1)$ e $(2, 0)$, respectivamente. Substituindo os polinômios $g = a_{00} + a_{10}x + a_{01}y + a_{11}xy$ e $h = b_{00} + b_{10}x + b_{20}x^2$ na equação (3.2), constrói-se o sistema linear*

$$\begin{bmatrix} -1 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 & 2 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \\ b_{00} \\ b_{10} \\ b_{20} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

A solução desse problema é o subespaço vetorial de $\mathbb{Q}^7$ gerado pelo vetor

$$\begin{bmatrix} 0 & 0 & 2 & 0 & 1 & 0 & 0 \end{bmatrix}^T$$

Logo, temos $G = \{2x\}$ *e, como dim* $G = 1$*, segue que* $G' = G$ *e* f *é absolutamente irredutível.*

Esse resultado já estabelece uma relação entre G' e os fatores de f, o que nos motiva a investigar a sua estrutura com maior atenção. Nesse sentido, o problema de recuperar G' a partir de G é extremamente importante, e será tratado a seguir. Em primeiro lugar, veremos uma propriedade que associa elementos de G a fatores absolutamente irredutíveis de f.

Teorema 3.1.4. *Seja* $\bar{f}$ *um fator irredutível de* f *em* $F[x, y]$ *que é produto de* s *fatores absolutamente irredutíveis* $f_1, ..., f_s$ *em* $\bar{F}[x, y]$*. Então, existem* $g_1, ..., g_s$ *em* G *com a propriedade de que, para todo* $g = \sum_{i=1}^{s} \alpha_i g_i$*, com* $\alpha_1, ..., \alpha_s$ *em* F*, há uma única matriz* $A = (a_{ij}) \in F^{s\times s}$ *satisfazendo*

$$gg_i \equiv \sum_{j=1}^{s} a_{ij} g_j \frac{\partial f}{\partial x} \ mod \ f.$$

Demonstração

Conforme feito no teorema (3.1.1) , obtêm-se s homomorfismos distintos $\sigma_1, ..., \sigma_s$ de K em $\bar{F}$ que restritos a F são a identidade, onde K é a extensão de F originada pela adjunção dos coeficientes de f_1 (ou, equivalentemente, de f_2, f_3, ... ou f_s). Mas essa extensão é finitamente gerada e separável, de forma que existe um elemento primitivo $\alpha \in \bar{F}$ tal que

$$K = F(\alpha) = \{a_0 + a_1\alpha + ... + a_{s-1}\alpha^{s-1};\ a_0, a_1, ..., a_{s-1} \in F\}.$$

Além disso, a dimensão s desse espaço vetorial coincide com o número de automorfismos distintos de $\bar{F}$ que fixam F, que denotaremos por $\sigma_1, ..., \sigma_s$.

Utilizamos o operador traço para definir

$$g_i = \sum_{j=1}^{s} \sigma_j(\alpha^i E_1) = \sum_{j=1}^{s} \sigma_j(\alpha)^i \sigma_j E_1,\ i = 1, ..., s.$$

Esses elementos g_i nada mais são do que os e_i's do teorema (3.1.1) e, conforme vimos nessa ocasião, $g_i \in G$, $i = 1, .., s$.

Por um lado,

$$\begin{aligned} gg_i &= (\sum_{j=1}^{s} \alpha_j \sum_{k=1}^{s} \sigma_k(\alpha)^j \sigma_k E_1)(\sum_{k=1}^{s} \sigma_k(\alpha)^i \sigma_k E_1) \\ &= (\sum_{k=1}^{s} \sum_{j=1}^{s} (\alpha_j \sigma_k(\alpha)^j) \sigma_k E_1)(\sum_{k=1}^{s} \sigma_k(\alpha)^i \sigma_k E_1). \end{aligned}$$

Mas homomorfismos σ_k distintos levarão E_1 a E_k's distintos, de forma que $\sigma_k E_1 \sigma_j E_1 \equiv 0 \ mod \ f$ sempre que $k \neq j$. Segue que

$$gg_i \equiv \sum_{k=1}^{s} (\sum_{j=1}^{s} \alpha_j \sigma_k(\alpha)^{j+i}) \sigma_k^2 E_1 \ mod \ f. \tag{3.5}$$

Por outro lado, $g_j \frac{\partial f}{\partial x} = (\sum_{k=1}^{s} \sigma_k(\alpha)^j \sigma_k E_1)(\sum_{k=1}^{s} E_k)$. Observando que $\sigma_k(E_1)E_l \equiv 0 \ mod \ f$, se $\sigma_k(E_1) \neq E_l$, vem $g_j \frac{\partial f}{\partial x} \equiv \sum_{k=1}^{s} \sigma_k(\alpha)^j \sigma_k^2 E_1 \ mod \ f$. Logo, devemos determinar $A = (a_{ij})$ satisfazendo

$$\sum_{j=1}^{s} a_{ij} g_j \frac{\partial f}{\partial x} \equiv \sum_{k=1}^{s} (\sum_{j=1}^{s} a_{ij} \sigma_k(\alpha)^j) \sigma_k^2 E_1 \ mod \ f. \tag{3.6}$$

Utilizando (3.5) e (3.6), escreve-se $gg_i \equiv \sum_{j=1}^{s} a_{ij} g_j \frac{\partial f}{\partial x}$ forma matricial. A existência dos a_{ij} estará condicionada à solução do seguinte problema:

$$\begin{bmatrix} \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+1} & . & \sum_{j=1}^{s} \alpha_j \sigma_s(\alpha)^{j+1} \\ . & . & . \\ \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+s} & . & \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+s} \end{bmatrix} \begin{bmatrix} \sigma_1(E_1)^2 \\ . \\ \sigma_s(E_1)^2 \end{bmatrix} \equiv$$

$$\begin{bmatrix} \sigma_1(\alpha) & . & \sigma_s(\alpha) \\ . & . & . \\ \sigma_1(\alpha)^s & . & \sigma_s(\alpha)^s \end{bmatrix} \begin{bmatrix} a_{11} & . & a_{1s} \\ . & . & . \\ a_{s1} & . & a_{ss} \end{bmatrix} \begin{bmatrix} \sigma_1(E_1)^2 \\ . \\ \sigma_s(E_1)^2 \end{bmatrix} \tag{3.7}$$

Mas a matriz

$$\begin{bmatrix} \sigma_1(\alpha) & . & \sigma_s(\alpha) \\ . & . & . \\ \sigma_1(\alpha)^s & . & \sigma_s(\alpha)^s \end{bmatrix}$$

é invertível, de forma que

$$\begin{bmatrix} \sigma_1(\alpha) & . & \sigma_s(\alpha) \\ . & . & . \\ \sigma_1(\alpha)^s & . & \sigma_s(\alpha)^s \end{bmatrix}^{-1} \begin{bmatrix} \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+1} & . & \sum_{j=1}^{s} \alpha_j \sigma_s(\alpha)^{j+1} \\ . & . & . \\ \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+s} & . & \sum_{j=1}^{s} \alpha_j \sigma_1(\alpha)^{j+s} \end{bmatrix}$$

é uma solução para A.

Se mostrarmos que $E_i^2 \ mod \ f$ são linearmente independentes sobre $\bar{F}$, segue que essa solução é única.

De fato, se $a_1, ..., a_r \in \bar{F}$ são tais que $\sum_{i=1}^{r} a_i E_i^2 \equiv 0 \ mod \ f$, existe $h \in \bar{F}[x, y]$ satisfazendo $\sum_{i=1}^{r} a_i (\frac{f}{f_i})^2 \frac{\partial f_i}{\partial x}^2 = fh$.

Então, para $k \in \{1, ..., r\}$,

$$a_k (\frac{f}{f_k})^2 \frac{\partial f_k}{\partial x}^2 = fh - \sum_{i \neq k} a_i (\frac{f}{f_i})^2 \frac{\partial f_i}{\partial x}^2 .$$

Note que f_k divide o polinômio da direita, pois divide todos os seus termos. Por outro lado, $mdc(f_k, (\frac{f}{f_k})^2) = 1$ e $mdc(f_k, \frac{\partial f_k}{\partial x}^2) = 1$, já que $mdc(f, \frac{\partial f}{\partial x}) = 1$. Esses fatos acima implicam que $a_k (\frac{f}{f_k})^2 \frac{\partial f_k}{\partial x}^2 = 0$, isto é, $a_k = 0$.

Para concluir, observamos que, como o problema linear (3.7) é um sistema linear possível com coeficientes no corpo F, sua solução (única) certamente estará em F. □

Procuraremos agora estabelecer uma forma de recíproca para o teorema acima. De fato, demonstraremos que os conjuntos $\{g_1, ..., g_s\}$ que satisfazem essa propriedade estão em G'.

Teorema 3.1.5. *Se $\{g_1, ..., g_s\} \subset G$ é tal que, para cada $k \in \{1, ..., s\}$, existe $A_k = (a_{ij}^k) \in F^{s \times s}$ satisfazendo*

$$g_k g_i \equiv \sum_{j=1}^{s} a_{ij}^k g_j \frac{\partial f}{\partial x} \ mod \ f,$$

então $\{g_1, ..., g_s\} \subset G'$.

Tal conjunto será denominado solução do teste matricial s-dimensional associado a G.

Demonstração

Seja $k \in \{1, 2, ..., s\}$ e consideremos a matriz $A_k = (a_{ij}^k)$ do teorema. Dispomos da seguinte equação na forma matricial:

$$\begin{bmatrix} g_k g_1 \\ g_k g_2 \\ . \\ g_k g_s \end{bmatrix} \equiv A_k \begin{bmatrix} g_1 \frac{\partial f}{\partial x} \\ g_2 \frac{\partial f}{\partial x} \\ . \\ g_s \frac{\partial f}{\partial x} \end{bmatrix} \ mod\ f, \text{ de modo que}$$

$$(g_k I_{s\times s} - \frac{\partial f}{\partial x} A_k) \begin{bmatrix} g_1 \\ g_2 \\ . \\ g_s \end{bmatrix} \equiv 0\ mod\ f$$

Mas, se (f) denota o ideal gerado por f em $F[x, y]$, a estrutura $F[x, y]/(f)$ é, em geral, apenas um anel, de forma que não valem alguns resultados conhecidos da Álgebra Linear. Seja então $f = \hat{f}_1 ... \hat{f}_t$ a fatoração de f em fatores irredutíveis racionais (ou seja, sobre $F[x, y]$). Logo, para $j = 1, 2, ..., t$ temos equações

$$(g_k I_{s\times s} - \frac{\partial f}{\partial x} A_k) \begin{bmatrix} g_1 \\ g_2 \\ . \\ g_s \end{bmatrix} \equiv 0\ mod\ \hat{f}_j,$$

e agora, como $(\hat{f}_j)$ é um ideal primo de $F[x, y]$, a estrutura $F[x, y]/(\hat{f}_j)$ é um domínio de integridade. Então, o vetor $[g_1, ..., g_s]$ é nulo, ou a matriz $(g_k I_{s\times s} - \frac{\partial f}{\partial x} A_k)$ é singular em $F[x, y]/(\hat{f}_j)$. Sejam $\Lambda_1 = \{j \in \{1, 2, ..., t\}; [g_1, ..., g_s] = [0, ..., 0]\ mod\ \hat{f}_j\}$ e $\Lambda_2 = \{1, 2, ..., t\} \backslash \Lambda_1$. O vetor $[g_1, ..., g_s]$ só será nulo se $\hat{f}_j$ dividir todos os seus elementos, e, como $grau_x(g_i) < grau_x(f)$, o conjunto Λ_2 não é vazio. Sem perda de generalidade, sejam $\Lambda_1 = \{1, 2, ..., t_1\}$, $\Lambda_2 = \{t_1 + 1, ..., t\}$, $0 \leq t_1 < t$.

Para cada j em Λ_2, a matriz $(g_k I_{s\times s} - \frac{\partial f}{\partial x} A_k)$ é singular módulo $\hat{f}_j$, logo

$$det(g_k I_{s\times s} - \frac{\partial f}{\partial x} A_k) \equiv 0 \ mod \ \hat{f}_j$$

e, em particular, o polinômio característico $char(\frac{\partial f}{\partial x} A_k)(z) = (\frac{\partial f}{\partial x})^s char(A_k)(z/\frac{\partial f}{\partial x})$ se anula quando aplicamos $z = g_k$. Sejam $\alpha_1, ..., \alpha_s$ as raízes (possivelmente repetidas) do polinômio $char(A_k)(z)$ em seu corpo de decomposição. Do que acabamos de comentar, conclui-se que

$$(g_k - \alpha_1 \frac{\partial f}{\partial x})...(g_k - \alpha_s \frac{\partial f}{\partial x}) = (\frac{\partial f}{\partial x})^s char(A_k)(g_k/\frac{\partial f}{\partial x}) \equiv 0 \ mod \ \hat{f}_j.$$

Mas $\frac{\partial f}{\partial x} = \sum_{i=1}^{r} E_i$, onde r é o número de fatores absolutamente irredutíveis de f, de forma que

$$(g_k - \alpha_1 \sum_{i=1}^{s} E_i)...(g_k - \alpha_s \sum_{i=1}^{s} E_i) \equiv 0 \ mod \ \hat{f}_j,$$

isto é, $\hat{f}_j$ divide $(g_k - \alpha_1 \sum_{i=1}^{s} E_i)...(g_k - \alpha_s \sum_{i=1}^{s} E_i)$. Sejam agora $\bar{\Lambda_2} = \{1, ..., r_1\}$ (sem perda de generalidade), $1 \leq r_1 \leq r$, o conjunto dos índices associados aos fatores absolutamente irredutíveis dos elementos em Λ_2 e $\{P_1, ..., P_s\}$ uma partição de $\bar{\Lambda_2}$ tal que $l \in P_j \Rightarrow f_l$ divide $g_k - \alpha_j \sum_{i=1}^{s} E_i$.

Se $l \in P_1$, então f_l divide $g_k - \alpha_1 \sum_{i=1}^{s} E_i$, e, como todos os E_j's, a exceção de E_l, são divisíveis por f_l, vem que $g_k = \alpha_1 E_l + q f_l$, para algum $q \in F[x, y]$ cujo grau na variável x é inferior a $n - 1$. Pelo mesmo argumento, obtemos $g_k = \alpha_1 \sum_{i\in P_1} E_i + q \prod_{i\in P_1} f_i$, com $q \in F[x, y]$ satisfazendo $grau_x(q) < n - 1 - \sum_{i\in P_1} grau_x(f_i)$. Repete-se o procedimento para todos os demais elementos da partição para obter $g_k = \alpha_1 \sum_{i\in P_1} E_i + ... + \alpha_s \sum_{i\in P_s} E_i + \bar{q} \prod_{i\in P_1\cup...\cup P_s} f_i$, para algum $\bar{q} \in F[x, y]$, com $grau_x(\bar{q}) < n - 1 - \sum_{i\in P_1\cup...\cup P_s} grau_x(f_i)$. Mas o elemento $h = \prod_{i\in\Lambda_1} \hat{f}_i$ divide tanto g_k quanto E_j, $\forall \ j \in \bar{\Lambda_2}$. Logo, h divide $\bar{q} \prod_{i\in P_1\cup...\cup P_s} f_i = \bar{q} \prod_{i\in\Lambda_2} \hat{f}_i$, e, pelo fato de que $h = \prod_{i\in\Lambda_1} \hat{f}_i$ e o último produtório são relativamente primos, segue que h divide $\bar{q}$. Como $grau_x(h) = n - \sum_{i\in\bar{\Lambda_2}} grau_x(f_i) > grau_x(\bar{q})$, temos que $\bar{q} = 0$. Estabelecemos portanto que $g_k \in G'$, para k arbitrário em $\{1, ..., s\}$, o que conclui o teorema. □

Veremos que, conhecendo as soluções dos testes matriciais s-dimensionais, será possível obter G'.

Corolário 3.1.6. *Sejam $B_1, ..., B_s$ subconjuntos linearmente independentes maximais das soluções do teste matricial i-dimensional associado a G, $1 \leq i \leq s$. Então, se todos os fatores irredutíveis de f sobre $F[x, y]$ forem produto de no máximo s fatores absolutamente irredutíveis, G' é o subespaço vetorial de G gerado por $\bigcup_{i=1}^{s} B_i$.*

Demonstração

O teorema (3.1.5) garante que $B_i \subset G'$, $\forall\ i$, de forma que a contenção $< \bigcup_{i=1}^{s} B_i > \subset G'$ vale.

Reciprocamente, suponha que $f_1, ..., f_t$ são os fatores absolutamente irredutíveis de um mesmo fator irredutível racional $\bar{f}$ de f. Sejam $E_1 = \frac{f}{f_1}\frac{\partial f_1}{\partial x}$ e $\alpha \in \bar{F}$ um elemento primitivo de K, a extensão algébrica separável de F obtida por adjunção dos coeficientes de f_1. Pela demonstração do teorema (3.1.1), existem elementos $e_1, ..., e_t$, $e_i = \sum_{j=1}^{t} \sigma_j(\alpha^i E_1)$, que integram uma base de G' (lembre que os σ_i's são homomorfismos de K em $\bar{F}$ que coincidem com a identidade em F). Mas a prova do teorema (3.1.4) mostra que $\{e_1, ..., e_t\}$ é uma solução para o teste t-dimensional. Como, por hipótese, $t \leq s$, $\{e_1, ..., e_t\} \subset B_t$, o que conclui a demonstração. □

A teoria desenvolvida acima nos fornece um algoritmo para computar uma base de G', pois identifica elementos de G' (teorema 3.1.5) e determina uma condição de parada (último corolário).

Algoritmo 3.1.7. *Base para G'*

Entrada: *Um polinômio f sobre $F[x,y]$, onde F é um corpo finito, uma base B para G, o espaço nulo do sistema de Gao associado a f, e uma cota s no número de fatores absolutamente irredutíveis que compõem os fatores irredutíveis de f sobre $F[x,y]$.*

Saída: *Uma base B' para G'.*

1. $B' \leftarrow \emptyset$
2. *para* $k = 1, ..., s$ *faça*
3. *para todo subconjunto* $\{h_1, ..., h_k\}$ *de cardinalidade* k *de combinações lineares de elementos de* G *faça*
4. *se, para cada* $l \in \{1, ..., k\}$, *existe* $A_l = (a_{ij}^l) \in F^{k \times k}$ *tal que* $h_l h_i \equiv \sum_{j=1}^{k} a_{ij}^l h_j \frac{\partial f}{\partial x}$ *mod* f *adicione* $\{h_1, ..., h_k\}$ *a* B', *removendo os fatores necessários para manter os elementos de* B' *linearmente independentes*
5. *devolva* B'

Retomaremos agora as idéias originais de Gao para relacionar o espaço vetorial G' aos fatores de f. Veremos como os elementos de G' serão responsáveis pela quebra de f em seus fatores (absolutamente) irredutíveis.

Uma solução $g \in G'$ é dita trivial se for um múltiplo escalar de $\frac{\partial f}{\partial x}$. Pelo que vimos anteriormente, existe uma solução não trivial em G' se, e somente se, $r > 1$, ou seja, f não é absolutamente irredutível.

Proposição 3.1.8. *Para todo $g \in G'$ não trivial, $f = \prod_{\lambda \in \bar{F}} mdc(f, g - \lambda \frac{\partial f}{\partial x})$ é uma fatoração própria de f sobre $\bar{F}$.*

Demonstração

Seja $g \in G'$. Pelo teorema (3.1.1), existem $\lambda_i \in \bar{F}$ com $g = \sum_{i=1}^{r} \lambda_i E_i$, lembrando que $E_i = \frac{f}{f_1}\frac{\partial f_i}{\partial x}$, $i = 1, ..., r$. Lembremos também que $\frac{\partial f}{\partial x} = \sum_{i=1}^{r} E_i$, logo

$$g - \lambda\frac{\partial f}{\partial x} = \sum_{i=1}^{r}(\lambda_i - \lambda)E_i.$$

Analisemos $mdc(f, g - \lambda\frac{\partial f}{\partial x})$ à medida que λ varia em $\bar{F}$:

Se $\lambda = \lambda_j$, para certo j, $g - \lambda\frac{\partial f}{\partial x} = g - \lambda_j\frac{\partial f}{\partial x} = \sum_{i\neq j}(\lambda_i - \lambda_j)E_i$. Mas f_j divide E_i, $\forall\ i \neq j$, de forma que $g - \lambda_j\frac{\partial f}{\partial x}$ é divisível por f_j. Conseqüentemente, f_j divide $mdc(f, g - \lambda_j\frac{\partial f}{\partial x})$.

Se $\lambda \neq \lambda_j$, f_j não divide $mdc(f, g - \lambda\frac{\partial f}{\partial x})$, pois, dado $i \in \{1, ..., r\}$, f_j divide E_i, se $i \neq j$, e f_j não divide E_j, já que $mdc(f, \frac{\partial f}{\partial x}) = 1$, o que estabelece a afirmação. Em particular, se $\lambda \neq \lambda_i$, $\forall\ i$, então $mdc(f, g - \lambda\frac{\partial f}{\partial x}) = 1$.

Portanto, temos que $f = \prod_{\lambda\in\bar{F}} mdc(f, g - \lambda\frac{\partial f}{\partial x})$ é uma fatoração de f sobre $\bar{F}$. Ela é própria porque existem índices $i, j \in \{1, ..., r\}$ tais que $\lambda_i \neq \lambda_j$, caso contrário $g = \lambda_1 f$, isto é, g é trivial. □

Para quaisquer dois fatores absolutamente irredutíveis f_i e f_j de f, dizemos que eles são separados por g se eles estiverem em fatores diferentes na fatoração própria induzida por g, que foi definida acima. De fato, a proposição acima garante que g separa f_i de f_j se, e somente se, $\lambda_i \neq \lambda_j$. Um conjunto de elementos $g_1, ..., g_l \in G$ é dito um conjunto de separação para f se qualquer par de fatores absolutamente irredutíveis de f é separado por algum g_i, $1 \leq i \leq l$. Uma fatoração completa para f pode ser recuperada se conhecermos um conjunto de separação para f. O seguinte algoritmo realiza essa tarefa:

Algoritmo 3.1.9.

Entrada: *Um conjunto de separação finito C para f e uma fatoração* $Fat_c = \{f_1^c, ..., f_{n_c}^c\}$ *para cada* $c \in C$

Saída: *Os fatores absolutamente irredutíveis* $f_1, ..., f_r$ *de* f.

1. $S \leftarrow \emptyset$, $G \leftarrow \cup_{c \in C} Fat_c$.
2. *enquanto* $G \neq \emptyset$ *faça*
   escolha $g \in G$, $G \leftarrow G \backslash \{g\}$
3. *para todo* $h \in G$ *faça*
4. *se* $mdc(g,h) \neq 1 \in \bar{F}[x,y]$ *então*
5. *se* $mdc(g,h) = h$
   então
   $G \leftarrow G \cup \{g/h\}$, *vá para* 2
   senão
   $G \leftarrow G \backslash \{h\}$
6. *se* $mdc(g,h) \neq g$ *então*
   $G \leftarrow G \cup \{mdc(g,h), g/mdc(g,h), h/mdc(g,h)\}$
   vá para 2
7. $S \leftarrow S \cup \{g\}$
8. *devolva* S

O algoritmo acima é intuitivo, portanto demonstraremos sua validade sem apresentar exemplos, dado que sua aplicação aparecerá em exemplos posteriores.

Proposição 3.1.10. *O algoritmo anterior determina corretamente um conjunto de fatores absolutamente irredutíveis de* f.

Demonstração

Em primeiro lugar, observemos que todos os elementos de S são relativamente primos com elementos de G. Isso é trivialmente verificado no início do

algoritmo e suporemos que essa afirmação valha antes de uma determinada passagem por 2. Mas, ao escolhermos g no passo 2, há apenas duas maneiras de que ele seja incluído em S. A primeira ocorre no caso em que $mdc(g,h) = 1$, para todo $h \in G$. A segunda ocorre quando $mdc(g,h) = g$ sempre que $mdc(g,h) \neq 1$, e, portanto, esses elementos h serão todos eliminados de G durante o passo 5. Isso estabelece nossa afirmação.

Em particular, os elementos em S são irredutíveis, pois, se f_i e f_j são fatores de $g \in G$, então f_i e f_j não dividem nenhum elemento contido em S pela afirmação anterior. Além disso, como fatores absolutamente irredutíveis só são eliminados de G quando forem incluídos em S, e C é um conjunto de separação para f, existe $h \in G$ tal que f_i divide h e f_j não divide h. Logo, $1 \neq mdc(g,h) \neq g$, e portanto g não é anexado a S, conforme nossa discussão anterior.

Só nos resta verificar que, a cada intervalo finito de passos, um elemento g é incluído em S, pois, pela invariância acima, temos que G será vazio assim que o último fator irredutível de f for anexado a S. Mas essa verificação decorre do fato que, a cada escolha de g em 2, g é retirado de G e os elementos adicionados a G têm grau total estritamente menor ao de g (aqui, $grau\ total(g) = max\{i+j$; o coeficiente de $x^i y^j$ não é nulo$\}$). Como G é finito no início do algoritmo, a quantidade $max\{grau\ total(g); g \in G\}$ é não-crescente e certamente decrescerá após um número finito de passagens por 2, já que cada elemento é composto por um número finito de fatores próprios, o que conclui a demonstração. $\square$.

O resultado que apresentamos nesse momento expressa a ligação entre G' e a fatoração de f em elementos irredutíveis e decorre diretamente de resultados já estabelecidos.

Corolário 3.1.11. *Qualquer base de G' é um conjunto de separação para f.*

Demonstração

Seja $\{g_1, ..., g_r\}$ uma base para G' sobre F. Da demonstração da proposição (3.1.8), g separa f_i de f_j se $\lambda_i \neq \lambda_j$ na expansão de g pelos E_i's. Mas $g_k = \sum_{i=1}^{r} \lambda_i^k E_i$,

para certos $\lambda_i^k \in \bar{F}$, $k = 1, ..., r$. Suponha, por absurdo, que tenhamos i, j distintos tais que $\lambda_i^k = \lambda_j^k$, $\forall\ k$.

Nesse caso, $\{g_1, ..., g_r\} \subset \ < \{E_k;\ k \notin \{i, j\}\}, E_i + E_j >_{\bar{F}}$, o que contradiz o fato de que $\{g_1, ..., g_r\}$ são linearmente independentes sobre $\bar{F}$, conforme atesta a demonstração do teorema (3.1.1). □

Corolário 3.1.12. *Se $g_1, ..., g_r$ é uma base para G' sobre F, então, para todo $g \in G'$, existe uma única matriz $A = (a_{ij}) \in F^{r\times r}$ satisfazendo*

$$gg_i \equiv \sum_{j=1}^{s} a_{ij} g_j \frac{\partial f}{\partial x}\ mod\ f.$$

Além disso, seja $E_g(x) = det(I_{r\times r}x - A)$ o polinômio característico da matriz A. Então, o número de fatores irredutíveis distintos de $mdc(f, g - \lambda\frac{\partial f}{\partial x})$ em $\bar{F}[x, y]$ é igual à multiplicidade de λ como raiz de $E_g(x)$.

Demonstração

Sejam $\{g_1, ..., g_r\}$ uma base para G' e $g \in G'$.

Vimos no teorema (3.1.1) que $\{g_1, ..., g_r\}$ são linearmente independentes também sobre $\bar{F}$, de forma que existe uma matriz invertível $B \in \bar{F}^{r\times r}$ tal que

$$\begin{bmatrix} g_1 \\ g_2 \\ . \\ g_r \end{bmatrix} = B \begin{bmatrix} E_1 \\ E_2 \\ . \\ E_r \end{bmatrix}$$

Além disso, pela definição de G', existem $\lambda_1, ..., \lambda_r \in \bar{F}$ tais que

$$g = \sum_{i=1}^{r} \lambda_i E_i.$$

Lembrando que $E_iE_j \equiv 0 \ mod \ f$ sempre que $i \neq j$ e que $\frac{\partial f}{\partial x} = \sum_{i=1}^{r} E_i$, obtemos

$$\begin{aligned} g \begin{bmatrix} g_1 \\ . \\ g_r \end{bmatrix} &= gB \begin{bmatrix} E_1 \\ . \\ E_r \end{bmatrix} = B \begin{bmatrix} gE_1 \\ . \\ gE_r \end{bmatrix} \\ &= B \begin{bmatrix} \sum_{i=1}^{r} \lambda_i E_i E_1 \\ . \\ \sum_{i=1}^{r} \lambda_i E_i E_r \end{bmatrix} \equiv B \begin{bmatrix} \lambda_1 E_1^2 \\ . \\ \lambda_r E_r^2 \end{bmatrix} \ mod \ f \end{aligned} \tag{3.8}$$

$$\begin{aligned} \frac{\partial f}{\partial x} \begin{bmatrix} g_1 \\ . \\ g_r \end{bmatrix} &= \frac{\partial f}{\partial x} B \begin{bmatrix} E_1 \\ . \\ E_r \end{bmatrix} = B \begin{bmatrix} \frac{\partial f}{\partial x} E_1 \\ . \\ \frac{\partial f}{\partial x} E_r \end{bmatrix} \\ &\equiv B \begin{bmatrix} E_1^2 \\ . \\ E_r^2 \end{bmatrix} \ mod \ f \end{aligned} \tag{3.9}$$

Seja, então,

$$A = B \begin{bmatrix} \lambda_1 & 0 & . & 0 \\ . & . & . & . \\ 0 & . & . & \lambda_r \end{bmatrix} B^{-1},$$

de onde segue, por (3.8) e (3.9), que

$$\begin{aligned} \frac{\partial f}{\partial x} A \begin{bmatrix} g_1 \\ . \\ g_r \end{bmatrix} &\equiv B \begin{bmatrix} \lambda_1 & 0 & . & 0 \\ . & . & . & . \\ 0 & . & . & \lambda_r \end{bmatrix} B^{-1} (B \begin{bmatrix} \lambda_1 E_1^2 \\ . \\ \lambda_r E_r^2 \end{bmatrix}) \ mod \ f \\ &\equiv B \begin{bmatrix} \lambda_1 & 0 & . & 0 \\ . & . & . & . \\ 0 & . & . & \lambda_r \end{bmatrix} \begin{bmatrix} E_1^2 \\ . \\ E_r^2 \end{bmatrix} \equiv g \begin{bmatrix} g_1 \\ . \\ g_r \end{bmatrix} \ mod \ f \end{aligned}$$

Logo, A é uma matriz satisfazendo as condições do corolário. A unicidade de A segue do fato que conjunto $\{E_1^2 \ mod \ f, ..., E_r^2 \ mod \ f\}$ é linearmente independente sobre $\bar{F}$, estabelecido no teorema (3.1.4).

A relação entre o número de fatores absolutamente irredutíveis distintos de $mdc(f, g - \lambda\frac{\partial f}{\partial x})$ e a multiplicidade de λ como raiz de $E_g(x)$ segue imediatamente da proposição (3.1.8). □

Esse último corolário garante que, conhecendo a fatoração de $E_g(x)$, recuperaremos fatores próprios de f, e eles serão absolutamente irredutíveis sempre que a multiplicidade da raiz correspondente de E_g for igual a um. No caso em que $E_g(x)$ não possui raízes mútiplas, isto é, for um polinômio separável, o conjunto unitário $\{g\}$ forma um conjunto de separação para f. A seguir, indicaremos como os fatores são recuperados.

Proposição 3.1.13. *Seja $\phi(x)$ um fator irredutível de $E_g(x)$ sobre F. Sejam $\lambda_1, ..., \lambda_t$ as raízes distintas de $\phi(x)$ em $\bar{F}$, e $g_i = mdc(f, g - \lambda_i\frac{\partial f}{\partial x})$, $i = 1, 2, ..., t$.*

Então,

(i) Se $\phi(x)$ é um fator simples (ou seja, com multiplicidade um) de $E_g(x)$, cada g_i, $1 \leq i \leq t$, é um fator absolutamente irredutível de f.

(ii) $h = g_1...g_t$ é um fator de f sobre F, irredutível quando $\phi(x)$ for um fator simples.

(iii) $h = mdc(f, \prod_{i=1}^{t}(g - \lambda_i\frac{\partial f}{\partial x})) = mdc(f, \frac{\partial f}{\partial x}^t \phi(g/\frac{\partial f}{\partial x}))$.

Demonstração

O item (i) é conseqüência imediata do corolário (3.1.12), pois o polinômio $g_i = mdc(f, g - \lambda_i\frac{\partial f}{\partial x})$ é um fator de f formado por apenas um fator absolutamente irredutível.

Itens (ii) e (iii): seja $h = \prod_{i=1}^{t}(g - \lambda_i\frac{\partial f}{\partial x})$. Como $\phi(x) = (x - \lambda_1)...(x - \lambda_t)$ sobre $\bar{F}$, temos $\phi(g/\frac{\partial f}{\partial x}) = (g/\frac{\partial f}{\partial x} - \lambda_1)...(g/\frac{\partial f}{\partial x} - \lambda_t)$ e $\frac{\partial f}{\partial x}^t \phi(g/\frac{\partial f}{\partial x}) = \prod_{i=1}^{t}(g - \lambda_i\frac{\partial f}{\partial x})$. Logo, vale que

$$h = mdc(f, \frac{\partial f}{\partial x}^t \phi(g/\frac{\partial f}{\partial x})) \tag{3.10}$$

Por outro lado, como $g - \lambda_i \frac{\partial f}{\partial x}$ e $g - \lambda_j \frac{\partial f}{\partial x}$ são relativamente primos se $i \neq j$, vale que

$$mdc(f, \prod_{i=1}^{t} g - \lambda_i \frac{\partial f}{\partial x}) = \prod_{i=1}^{t} mdc(f, g - \lambda_i \frac{\partial f}{\partial x}) = \prod_{i=1}^{t} g_i.$$

Concluímos que h é um fator de f que, por (3.10), está em $F[x, y]$. No caso em que ϕ é um fator simples de E_g, suponhamos, por absurdo, que h é redutível sobre $F[x, y]$, digamos $h = h_1 h_2$, com $h_1 = \prod_{i=1}^{t_1} g_i$ e $h_2 = \prod_{i=t_1+1}^{t} g_i$ $1 \leq t_1 < t$. Nesse caso,

$$\begin{aligned} h_1 &= \prod_{i=1}^{t_1} mdc(f, g - \lambda_i \frac{\partial f}{\partial x}) = mdc(f, \prod_{i=1}^{t_1} (g - \lambda_i \frac{\partial f}{\partial x})) \\ &= mdc(f, \frac{\partial f}{\partial x}^{t_1} \psi(g/\frac{\partial f}{\partial x})), \end{aligned}$$

onde $\psi(x) = \prod_{i=1}^{t_1}(x - \lambda_i)$. Segue que $\psi(x)$ é divisível por um polinômio não trivial com todos os seus coeficientes em F, o que contradiz a irredutibilidade de $\phi(x)$. □

Seja $L = F[t]/(\phi(t))$, $\phi(x)$ fator simples de E_g. Então $\alpha = t + (\phi(t))$ é uma raiz de ϕ em L, e $g_0 = mdc(f, g - \alpha \frac{\partial f}{\partial x})$ é um fator absolutamente irredutível de f sobre L. Esse fator g_0 serve como fator genérico de h, pois cada fator absolutamente irredutível $g_1, g_2, ..., g_t$ de h pode ser obtido substituindo α pelas raízes de $\phi(x)$ em $\bar{F}$.

Isso nos leva ao seguinte algoritmo para fatoração de polinômios em duas variáveis:

Algoritmo 3.1.14. *Algoritmo de Gao modificado*

Entrada: *Um corpo F, $f \in F[x,y]$, satisfazendo $mdc(f, \frac{\partial f}{\partial x}) = 1$, onde (m,n) é o grau de f em x e y, respectivamente.*

Saída: *Duas listas: RL para a lista de todos os fatores racionais irredutíveis de f. AL para a lista dos fatores absolutamente irredutíveis de f, dois a dois não algebricamente conjugados sobre F.*

1. $C \leftarrow \emptyset$
2. *construa o sistema linear de Gao e encontre uma base G para o seu espaço nulo sobre F*
3. *determine uma base $\{g_1, ..., g_r\}$ para o subespaço vetorial G' de G pelo algoritmo (3.1.7) se $r = 1$, então devolva $RL = \{f\}$ e $AL = \{[f, x]\}$*
4. *para $i = 1, 2, ..., r$*
5. *calcule $E_{g_i}(x)$ como no corolário (3.1.12)*
6. *fatore $E_{g_i}(x)$ sobre F.*
   $f_0 \leftarrow f$, o polinômio ainda a ser fatorado
7. *para cada fator simples $\phi(x)$ de $E_{g_i}(x)$,*
   calcule a multiplicidade $mult$ de ϕ como fator de E_{g_i}
   calcule $f_1 = mdc(f, g - \lambda\frac{\partial f}{\partial x})$ em $L[x,y]$, onde $L = F[t]/(\phi(t))$ e λ é a classe de congruência de t, isto é, uma raiz de $\phi(t)$ em L
   calcule $h_1 = mdc(f_0, \frac{\partial f}{\partial x}^t \phi(g/\frac{\partial f}{\partial x})) \in F[x,y]$, onde $t = grau\ \phi(x)$, e
   adicione $[h_1, f_1, \phi, mult]$ a C
   $f_0 \leftarrow f_0/h_1$
8. *utilize uma adaptação do algoritmo (3.1.9) para obter as listas RL e AL de fatores irredutíveis racionais e absolutos de f, reciprocamente*
9. *devolva as listas RL e AL*

Observações

1. Para descrever um fator irredutível g de f em $\bar{F}[x, y]$, deve-se especificar uma extensão finita de F que contenha os coeficientes de g. Tal extensão pode ser representada na forma $F[t]/(\phi(t))$, para certo polinômio irredutível $\phi(t) \in F[t]$. No algoritmo, denotamos por $[g, \phi(x)]$ tal fator e sua respectiva extensão.

2. O algoritmo de Gao modificado determina todos os fatores irredutíveis de f sobre $F[x, y]$ e, para cada um desses fatores, um fator g absolutamente irredutível. Obteremos uma lista de fatores absolutamente irredutíveis que, dois a dois, não são algebricamente conjugados. Para obter a fatoração absolutamente irredutível de f, basta determinar os fatores algebricamente conjugados aos elementos da lista.

3. O corolário (3.1.11) assegura que uma base $\{g_1, ..., g_r\}$ para G' fornece uma fatoração completa de f sobre $\bar{F}$. Para obtê-la, é necessária uma adaptação do algoritmo (3.1.9): dispomos de dois dados adicionais, que são o número de fatores absolutamente irredutíveis que devemos encontrar (a dimensão r de G') e o número de fatores irredutíveis e absolutamente irredutíveis contidos em cada fator de C. De fato, armazenamos os elementos de C na forma $[h_1, f_1, \phi, mult]$, o que nos informa que h_1 está em $F[x, y]$ e tem um fator f_1 em $L[x, y]$, onde $L = F[t]/(\phi(t))$. Informa-nos também que os demais fatores que compõem h_1 são algebricamente conjugados a f_1 na extensão de F determinada por ϕ e que h_1 tem fatoração absolutamente irredutível formada por $mult$ fatores. Portanto, o algoritmo (3.1.9) pode ser inicializado com a inclusão de todos os fatores irredutíveis que conhecemos a RL, quando racionais, e a AL, quando absolutos. Para pares $[h_1, f_1, \phi_1, m_1]$ e $[h_2, f_2, \phi_2, m_2]$, iniciamos calculando o máximo divisor comum de h_1 e h_2 em $F[x, y]$ e, somente no caso em que o resultado for diferente de um é que precisaremos computar máximos divisores comuns em $K[x, y]$, para alguma extensão finita K de F em que todos os fatores absolutamente irredutíveis envolvidos (f_1, f_2, e seus elementos algebricamente conjugados) estejam bem definidos. A única informação que será perdida após o primeiro passo é o número $mult$ de fatores.

4. Esse algoritmo requer que obtenhamos G' a partir de G. Isso acarreta dois problemas. O primeiro diz respeito à aplicabilidade do algoritmo: só sabemos recuperar G' de G para corpos finitos. O segundo se relaciona ao tempo de computação. Como o algoritmo para determinar G' tem comportamento exponencial, isso se reflete no tempo de computação do Algoritmo de Gao modificado.

Exemplo 3.1.15. *Vamos novamente recorrer ao exemplo que utilizamos no capítulo um, em que desejávamos fatorar o polinômio*

$$f(x,y) = x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1$$

em $F_2[x,y]$.

O passo 1 *se destina à inicialização das variáveis do algoritmo. No passo* 2*, construímos a matriz do problema de Gao associado a* f*, de ordem igual a* $((m+1)n + (n+1)m) \times 4mn$*, isto é,* 60×100 *em nosso exemplo. Calculamos em seguida uma base* G *para o seu espaço nulo, por exemplo* $G = \{1+y+y^2+x^3y^4+x^3y^5, xy^4+xy^5+x^2y^3+x^3y^2+x^4y^2, y^3+y^4+xy^2+x^2y+x^3y, x^3y^2+x^3y^3+x^4y^2, xy^2+xy^3+x^2y+x^3y, y+y^2+xy, x^2y^3+x^2y^4+x^3y^2+x^4y^2, x^2y+x^2y^2+x^3y, 1+y+y^2+x^4y^4\}$*. Note que a dimensão obtida foi* 9*, logo é claro que* G' *e* G *não coincidem, pois, como* f *tem grau* $m = 5$ *na variável* x *e todos os seus fatores dependem de* x *(já que* $mdc(f, \frac{\partial f}{\partial x}) = 1$*), não pode haver mais do que cinco fatores absolutamente irredutíveis em* f*.*

O passo 3 *se destina a calcular* G' *a partir de* G*. Para tanto, utilizaremos o algoritmo (3.1.7). A cota para o número* s *de testes a serem feitos será* $m = 5$*. O teste de dimensão* 1 *nos dá* $B' = B_1 = \{1+y+y+x^4y^4, y+y^2+xy\}$*. Para* $k = 2$*, há soluções* $B_2 = \{1+y+y+x^4y^4, y+y^2+xy\}$*, mas não há elementos linearmente independentes aos que já estão em* B'*. O teste de dimensão* 3 *não tem nenhuma solução, enquanto que, para dimensão* 4*, obtemos* $B_4 = \{y+y^2+xy, xy^2+xy^3+x^2y^2, x^3y^3+x^2y^3+x^2y^4, y+y^2+x^3y^4+x^3y^5+xy+x^4y^4\}$*. Os três últimos polinômios são linearmente independentes aos polinômios atualmente em* B'*, de forma que são adicionados a esse conjunto e* $B' = \{y+y^2+xy, 1+y+y^2+x^4y^4, xy^2+xy^3+$

$x^2y^2, x^3y^3 + x^2y^3 + x^2y^4, y + y^2 + x^3y^4 + x^3y^5 + xy + x^4y^4\}$. *O teste de dimensão* 5 *tem soluções compostas por polinômios linearmente dependentes aos de* B'*, logo não são adicionadas. O passo* 3 *se encerra então com uma base para* G'

$$B' = \{y+y^2+xy, 1+y+y^2+x^4y^4, xy^2+xy^3+x^2y^2, x^3y^3+x^2y^3+x^2y^4, y+y^2+x^3y^4+x^3y^5+xy+x^4y^4\}.$$

Em particular, f *tem cinco fatores absolutamente irredutíveis.*

Os passos $4, 5, 6$ *e* 7 *recuperam uma fatoração irredutível para cada um dos elementos da base:*

$$\begin{aligned}
C_1 &= \{[x+y+1, x+y+1, x, 1], [x^4y^4 + xy + 1, x^4y^4 + xy + 1, x + 1, 4]\},\\
&\quad \textit{pois } \phi_1(x) = x(x+1)^4\\
C_2 &= \{[x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1,\\
&\quad x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1, x + 1, 5\},\\
&\quad \textit{pois } \phi_2(x) = (x+1)^5\\
C_3 &= \{[x+y+1, x+y+1, x, 1], [x^4y^4 + xy + 1, xy + \lambda, x^4 + x + 1, 1]\},\\
&\quad \textit{pois } \phi_3(x) = x(x^4 + x + 1)\\
C_4 &= \{[x+y+1, x+y+1, x, 1], [x^4y^4 + xy + 1, xy + \lambda, x^4 + x + 1, 1]\},\\
&\quad \textit{pois } \phi_4(x) = x(x^4 + x + 1)\\
C_5 &= \{[x+y+1, x+y+1, x, 1], [x^4y^4 + xy + 1, xy + \lambda^3 + \lambda^2, x^4 + x^3 + 1, 1]\},\\
&\quad \textit{pois } \phi_5(x) = x(x^4 + x^3 + 1)
\end{aligned}$$

Note que os três últimos conjuntos já nos fornecem fatorações completas para f*, logo o passo* 8 *será encerrado antes que quaisquer cálculos sejam realizados. Finalmente, recuperamos os conjuntos* $RL = \{x + y + 1, x^4y^4 + xy + 1\}$ *e* $AL = \{[x + y + 1, x], [xy + \lambda, x^4 + x + 1]\}$*. Os fatores absolutamente irredutíveis que não aparecem expressamente no conjunto* AL *são os elementos algebricamente conjugados a* $xy+\lambda$*, onde* λ *é raiz de* $x^4 + x + 1$*, isto é,* $xy + \lambda^2$*,* $xy + \lambda + 1$ *e* $xy + \lambda^2 + 1$*. Portanto,*

$$x^5y^4+x^4y^5+x^4y^4+x^2y+xy^2+xy+x+y+1 = (x+y+1)(xy+\lambda)(xy+\lambda^2)(xy+\lambda+1)(xy+\lambda^2+1),$$

é a expansão de f em fatores absolutamente irredutíveis, com λ raiz de $x^4 + x + 1$. É evidente que a fatoração em elementos irredutíveis racionais é

$$x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1 = (x + y + 1)(x^4y^4 + xy + 1),$$

conforme visto nos exemplos anteriores.

Obtivemos portanto um algoritmo para fatoração de polinômios em duas variáveis sobre corpos finitos baseado no problema de Gao. A finitude do corpo é necessária para que G' seja recuperado com sucesso de G, mas veremos na próxima seção que um importante resultado de Gao retira essa restrição para corpos de característica zero ou suficientemente grande. Um segundo problema afeta a aplicabilidade do algoritmo: o modo proposto para recuperar G' de G não é muito eficiente nos casos em que G é um conjunto grande e deve ser melhorado. Outro passo ineficiente, embora menos problemático que o anterior, é a recuperação dos fatores irredutíveis a partir do conjunto C no passo 8 do algoritmo. Veremos, também na próxima seção, que esse passo será realizado com baixa probabilidade na prática.

3.2 As contribuições de Gao

O teorema que vem a seguir é o principal resultado do trabalho de Gao [Gao, 2003]. Ele estabelecerá uma restrição na característica do corpo F para que saibamos a priori que $G' = G$. Logo, poderemos aplicar o Algoritmo de Gao modificado omitindo o passo 3, de onde decorrerão duas vantagens imediatas. A primeira delas é evidente: a família de problemas que podem ser resolvidos pelo Algoritmo de Gao modificado é estendida. A segunda envolve a complexidade do algoritmo e será analisada mais adiante nessa seção.

Teorema 3.2.1. *Seja p a característica do corpo F e seja (m,n) o grau do polinômio $f \in F[x,y]$ em x e y, respectivamente. Supõe-se também que $mdc(f, \frac{\partial f}{\partial x}) = 1$. Se $p = 0$ ou $p > (2m-1)n$, então*

$$dim_F G = dim_F \bar{G} = r,$$

o número de fatores absolutamente irredutíveis de f. Em particular, $G' = G$.

Para a prova desse teorema, necessitaremos de um resultado em derivadas de funções algébricas sobre F. Veremos um polinômio em $F[x,y]$ como um polinômio em uma variável x com coeficientes em $F(y)$, o corpo das funções racionais em y. Portanto, será possível nos referirmos às raízes de f no fecho algébrico de $F(y)$, que são justamente as funções algébricas em y.

As derivadas de funções algébricas com respeito a y podem ser definidas univocamente. De fato, se α é separável sobre $F(y)$ e $T(x,y) \in F[x,y]$ é o polinômio minimal de α sobre $F(y)$, teremos $T(\alpha, y) = 0$ e a extensão D_y de $\frac{\partial}{\partial y}$ será definida por $D_y(\alpha) = -\frac{\partial}{\partial y}T(\alpha,y)/\frac{\partial}{\partial x}T(\alpha,y)$, com $\frac{\partial}{\partial x}T(\alpha,y) \neq 0$ pela separabilidade de α. Uma discussão mais completa dessa extensão consta no apêndice 2.

Utilizaremos um lema técnico.

Lema 3.2.2. *Seja $f \in F[x,y]$ com grau (m,n) e tal que $mdc(f, \frac{\partial f}{\partial x}) = 1$. Sejam β uma raiz de f no fecho algébrico de $F(y)$ e $\alpha = g(\beta,y)/\frac{\partial f}{\partial x}(\beta,y)$, onde $g \in F[x,y]$ tem grau menor ou igual a $(m-1,n)$. Suponha que a característica de F é igual a zero ou superior a $(2m-1)n$. Então, $D_y\alpha = 0$ implica que α é algébrico sobre F.*

Demonstração

Se $\alpha = 0$ nada há a fazer. Suponhamos $\alpha \neq 0$. O polinômio minimal de α sobre $F(y)$ pode ser escrito univocamente na forma

$$T(x,y) = v_0(y) + v_1(y)x + ... + v_l(y)x^l \in F[x,y],$$

onde $l \geq 1$, $v_0(y)v_l(y) \neq 0$ e $mdc(v_0(y), ..., v_l(y)) = 1$.

Como $T(\alpha, y) = 0$, é óbvio que $D_yT(\alpha, y) = 0$, isto é,

$$\frac{\partial}{\partial x}T(\alpha, y)\ D_y\alpha + \frac{\partial}{\partial y}T(\alpha, y) = 0.$$

Por hipótese, temos $D_y\alpha = 0$, de forma que a equação anterior resulta em

$$\frac{\partial}{\partial y}T(\alpha, y) = 0.$$

Utilizando a nossa expressão para T, isso é equivalente a

$$\frac{\partial v_0(y)}{\partial y} + ... + \frac{\partial v_l(y)}{\partial y}\alpha^l = 0.$$

Seja $Q(x, y) = \frac{\partial v_0(y)}{\partial y} + ... + \frac{\partial v_l(y)}{\partial y}x^l$. Mas, como T é polinômio minimal de α sobre $F(y)$ e $Q(\alpha, y) = 0$, sabemos que T divide Q. Mas o grau em y de Q é inferior ao de T, e portanto $\frac{\partial v_i(y)}{\partial y} = 0$, $i = 1, ..., l$.

Se a característica de F é zero, isso implica que $v_i(y) \in F$ para $i = 1, ..., l$ e α está em $\bar{F}$. Suponhamos que F tenha característica $p > 0$. Logo, cada $v_i(y)$ é da forma $v_i(y) = u_i(y^p)$, para certo $u_i \in F[y]$. Suponhamos, por absurdo, que $\alpha \notin \bar{F}$. Portanto, pelo menos um dos v_i's tem grau maior ou igual a um, conseqüentemente maior ou igual a p. Isso significa que o grau de $T(x, y)$ em y é de pelo menos p. Seja

$$M(x, y) = Res_z(f(z, y), x\frac{\partial f}{\partial x}(z, y) - g(z, y)) \in F[x, y]$$

Por um lado, se β é uma raiz de f no fecho algébrico de $F(y)$, vale que $\alpha\frac{\partial f}{\partial x}(\beta, y)$, que por hipótese coincide com $g(\beta, y)$. Portanto, β é uma raiz comum de $f(z, y)$ e $\alpha\frac{\partial f}{\partial x}(z, y) - g(z, y)$ em $F\bar{(}y)$. Da Teoria de Resultantes, vem que $M(\alpha, y) = 0$ e, como $T(x, y)$ é o polinômio minimal para α, $T(x, y)$ divide $M(x, y)$. Em particular, o grau em y de $M(x, y)$ é maior ou igual a p.

Por outro lado, pela definição de $M(x, y)$, é fácil ver que $grau_yM(x, y) \leq mn + (m - 1)n = (2m - 1)n$.

Como supusemos $p > (2m - 1)n$, isso nos leva a uma contradição, logo $\alpha \in \bar{F}$, o que conclui a demonstração do lema.

Demonstração do teorema

Conforme visto no teorema (3.1.1), $E_1, ..., E_r$ são elementos linearmente independentes de $\bar{G}$, e a cada um deles é possível associar um elemento em G linearmente independente dos demais. Portanto, é suficiente demonstrar que $\bar{G}$ é gerado por $E_1, ..., E_r$.

Seja $g \in \bar{G}$ e seja $h \in \bar{F}[x, y]$ satisfazendo o problema de Gao em conjunto com g. Consideraremos f, g, h como polinômios na variável x e coeficientes em $\bar{F}(y)$. Denotemos

$$f = u_m x^m + ... + u_1 x + u_0,$$

onde $u_i \in F[y]$ e $u_m \neq 0$.

Como $mdc(f, \frac{\partial f}{\partial x}) = 1$ em $F[x, y]$, o lema de Gauss estabelece que $mdc(f, \frac{\partial f}{\partial x}) = 1$ em $F(y)[x]$ e portanto f não possui raízes repetidas no fecho algébrico de $\bar{F}(y)$. Seja L o corpo de decomposição de f sobre $\bar{F}(y)$. Então, existem $c_i \in L$ distintos tais que $f = u_m \prod_{x=1}^{m}(x - c_i)$. Mas $grau_x g < grau_x f$, de onde vêm as decomposições em frações parciais

$$\frac{g}{f} = \sum_{i=1}^{m} \frac{a_i}{x - c_i}, \ \frac{h}{f} = \sum_{i=1}^{m} \frac{b_i}{x - c_i} + h_1, \tag{3.11}$$

onde $a_i = g(c_i, y)/\frac{\partial f}{\partial x}(c_i, y) \in L$, $b_i \in L$ e $h_1 \in F(y) \subset L$.

Como os operadores diferenciais $\frac{\partial}{\partial x}, \frac{\partial}{\partial y}$ em $F[x, y]$ podem ser estendidos univocamente a $L[x]$ (ver apêndice 2), segue que

$$D_y(\frac{g}{f}) = \sum_{i=1}^{m}(\frac{1}{x - c_i} D_y a_i + \frac{a_i}{(x - c_i)^2} D_y c_i)$$

$$D_x(\frac{h}{f}) = \sum_{i=1}^{m} \frac{-b_i}{(x - c_i)^2}$$

Logo,

$$D_y(\frac{g}{f}) = D_x(\frac{h}{f}) \Rightarrow \sum_{i=1}^{m} \frac{1}{x - c_i} D_y a_i + \frac{a_i D_y c_i + b_i}{(x - c_i)^2} = 0.$$

Mas os c_i's são todos distintos e tanto $D_y a_i$ quanto $a_i D_y c_i + b_i$ são independentes de x. Portanto, $D_y a_i = 0$, $i = 1, ..., m$. Aplicando o lema, segue que $a_i \in \bar{F}$, $i = 1, ..., m$. A continuidade do argumento depende da seguinte afirmação:

Afirmação: Se c_i e c_j são algebricamente conjugados sobre $\bar{F}(y)$, então a_i e a_j também o são.

A prova dessa afirmação é simples, pois, se c_i e c_j são algebricamente conjugados sobre $\bar{F}(y)$, existe um automorfismo $\sigma : F\bar{(}y) \to F\bar{(}y)$ tal que $\sigma(c_i) = c_j$ e σ coincide com o automorfismo identidade em $\bar{F}(y)$. Logo,

$$\begin{aligned}\sigma(a_i) &= \sigma(g(c_i, y)/\frac{\partial f}{\partial x}(c_i, y) = g(\sigma(c_i), y)/\frac{\partial f}{\partial x}(\sigma(c_i), y) \\ &= g(c_j, y)/\frac{\partial f}{\partial x}(c_j, y) = a_j\end{aligned}$$

Mas, se a_i e a_j são algebricamente conjugados sobre $\bar{F}(y)$, eles são iguais, pois estão em $\bar{F}$. Portanto, pelo fato acima, conclui-se que a_i e a_j coincidem para c_i e c_j na mesma classe de conjugação. Agora, agrupamos os termos de $\frac{g}{f}$ em (3.11) conforme eles estejam na mesma classe de conjugação. Como cada uma dessas classes corresponde a um fator irredutível de f sobre $\bar{F}(y)$, ou seja, a um dos f_i's, teremos

$$\begin{aligned}\frac{g}{f} &= \sum_{i=1}^{r} \lambda_i (\frac{1}{x - c_i^1} + ... + \frac{1}{x - c_i^{n_i}}) \\ &= \sum_{i=1}^{r} \frac{\lambda_i}{(x - c_i^1)...(x - c_i^{n_i})} \frac{\partial}{\partial x}(x - c_i^1)...(x - c_i^{n_i}) = \sum_{i=1}^{r} \frac{\lambda_i}{f_i} \frac{\partial f_i}{\partial x}.\end{aligned} \tag{3.12}$$

Portanto,

$$g = \sum_{i=1}^{r} \lambda_i \frac{f}{f_i} \frac{\partial f_i}{\partial x} = \sum_{i=1}^{r} \lambda_i E_i,$$

e a demonstração está concluída. □

Agora que se estendeu a aplicabilidade do algoritmo (3.1.14) a casos em que não é necessário calcular G' a partir de G, estudaremos a probabilidade de se encontrar uma fatoração completa de f sem necessidade do passo 8. Mais precisamente, se $\{g_1, ..., g_r\}$ é uma base de G', $S \subset F$ e $g = \sum_{i=1}^{r} a_i g_i$, para elementos

$a_1, ..., a_r$ escolhidos aleatoriamente em S, determinaremos a probabilidade de que E_g seja separável, e conseqüentemente, que a fatoração completa de f seja recuperada a partir de E_g. Necessitamos do seguinte lema:

Lema 3.2.3. *Separação de Probabilidade*

Seja A uma matriz $n \times m$ sem colunas repetidas sobre um determinado corpo. Suponha que S_i é um subconjunto de cardinalidade k desse corpo, $1 \leq i \leq n$. Escolha $a_i \in S_i$ de forma uniformemente aleatória e independente, $1 \leq i \leq n$, e definamos o vetor

$$\begin{bmatrix} v_1 & v_2 & . & v_m \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & . & a_n \end{bmatrix} A$$

Então, a probabilidade de que $v_1, ..., v_m$ sejam distintos é de pelo menos $1 - \frac{m(m-1)}{2k}$.

Demonstração

A prova desse resultado será feita por indução no número m de colunas da matriz A. Se $m = 1$, nada há a ser feito. Suponhamos que o lema seja válido para todas as matrizes com até $m - 1$ colunas, para certo $m > 1$.

Como $m > 1$ e não há colunas repetidas em A, existe uma linha da matriz A cujas entradas não são todas idênticas. Mas a ordem das linhas ou das colunas de A é insignificante para o resultado que desejamos estabelecer, logo podemos supor que a primeira linha de A tem elementos distintos e que A pode ser escrita na forma

$$A = \begin{bmatrix} \alpha_1 & . & \alpha_1 & ... & \alpha_t & . & \alpha_t \\ & A_1 & & ... & & A_t & \end{bmatrix}$$

onde $t \geq 2$, A_i possui $l_i \geq 1$ colunas, $l_1 + ... + l_t = m$ e os elementos $\alpha_1, ..., \alpha_t$ são todos distintos. Como A não conta com colunas repetidas, a mesma propriedade vale para cada uma das matrizes A_i, $1 \leq i \leq t$.

Mas o conjunto $\{v_1, ..., v_m\}$ consistirá de elementos distintos, se, e somente se as duas propriedades abaixo valem:

(a) para cada $i \in \{1, ..., t\}$, os elementos do vetor $[a_2 \quad . \quad a_n]A_i$ são todos distintos.

(b) para cada par $1 \leq i < j \leq t$ cada entrada do vetor $a_1[u_i \quad . \quad u_i] + [a_2 \quad . \quad a_n]A_i$ *é* distinta das entradas de $a_1[u_j \quad . \quad u_j] + [a_2 \quad . \quad a_n]A_j$.

Demonstremos que isso é verdade. Lembre que

$$\begin{bmatrix} v_1 & v_2 & . & v_m \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & . & a_n \end{bmatrix} \begin{bmatrix} \alpha_1 & . & \alpha_1 & ... & \alpha_t & . & \alpha_t \\ & A_1 & & ... & & A_t & \end{bmatrix}.$$

Assim, as l_1 primeiras entradas do vetor $[v_1 \ v_2 \quad . \quad v_m]$ são da forma $a_1\alpha_1 + \check{a}\ col_1A_1, ..., a_1\alpha_1 + \check{a}\ col_{l_1}A_1$, onde $\check{a} = [a_2 \ a_3 \quad . \quad a_n]$. Analogamente, as próximas l_2 entradas serão iguais a $a_1\alpha_2 + \check{a}\ col_1A_2, ..., a_1\alpha_2 + \check{a}\ col_{l_2}A_2$, e assim sucessivamente.

Portanto, para i fixo em $\{1, ..., t\}$, todos os elementos da forma $a_1\alpha_i + \check{a}col_j\ A_i$, $1 \leq j \leq l_i$ serão distintos se, e somente se, a propriedade (a) for válida. Por outro lado, todos os elementos da forma $a_1\alpha_i + \check{a}\ col_jA_i$ serão distintos de todos da forma $a_1\alpha_k + \check{a}\ col_lA_k$, $i \neq k$, se, e somente se, a propriedade (b) se verifica, o que estabelece a afirmação.

Mas, pela hipótese de indução, sabemos que

$$Prob([a_2 \quad . \quad a_n]A_i \text{tem entradas distintas}) \geq 1 - \frac{l_i(l_i-1)}{2k}, 1 \leq i \leq t,$$

onde $Prob$ denota probabilidade. Portanto,

$$\begin{aligned} Prob((a) \text{ é verdadeira}) &= Prob([a_2 \quad . \quad a_n]A_i \text{ tem entradas distintas, } i = 1, ..., m) \\ &= \prod_{i=1}^{t} Prob([a_2 \quad . \quad a_n]A_i \text{ tem entradas distintas}) \\ &\geq \prod_{i=1}^{t}(1 - \frac{l_i(l_i-1)}{2k}) \geq 1 - \sum_{i=1}^{t} \frac{l_i(l_i-1)}{2k}. \end{aligned}$$

A primeira igualdade decorre da independência na escolha dos a_i's. A última desigualdade, do fato que podemos supor $k \geq \frac{m(m-1)}{2}$ (caso contrário o enunciado do teorema é inócuo), e conseqüentemente $0 \leq \frac{l_i(l_i-1)}{2k} \leq 1$.

Agora, calcularemos a probabilidade condicional de (b) ser válido supondo a validade de (a), isto é, a probabilidade de que (b) valha para uma escolha qualquer de $a_2, ..., a_n$. Sejam i, j, $1 \leq i < j \leq t$, e w_1, w_2 colunas arbitrárias de A_i e A_j, respectivamente. Se

$$a_1 u_i + [a_2 \quad . \quad a_n] w_1 = a_1 u_j + [a_2 \quad . \quad a_n] w_2,$$

então

$$a_1 = [a_2 \quad . \quad a_n](w_2 - w_1)/(u_i - u_j),$$

já que $u_i \neq u_j$. Logo, a_1 deve evitar esses valores sempre que eles pertençam a S_1 e, como A_i, A_j possuem l_i, l_j colunas, respectivamente, o número de valores distintos da forma anterior é limitado por

$$l = \sum_{1 \leq i < j \leq t} l_i l_j.$$

Assim, como a_1 é escolhido de forma uniformemente aleatória, vale que

$$Prob((b) \text{ vale} | (a) \text{ vale}) \geq 1 - \frac{l}{k}.$$

Logo,

$$\begin{aligned} Prob(\{v_1, ..., v_m\} \text{ são distintos}) &= Prob((a) \text{ e } (b) \text{ valem}) \\ &= Prob((a) \text{ vale}) \cdot Prob((b) \text{ vale} | \ (a) \text{ vale}) \\ &\geq (1 - \sum_{i=1}^{t} \frac{l_i(l_i - 1)}{2k})(1 - \frac{l}{k}) \\ &\geq 1 - \sum_{i=1}^{t} \frac{l_i(l_i - 1)}{2k} - \frac{l}{k} = 1 - \frac{m(m-1)}{2k}, \end{aligned}$$

o que conclui a demonstração. □

Utilizando esse lema como ferramenta, estabeleceremos uma cota para o nosso problema:

Teorema 3.2.4. *Seja $f \in F[x,y]$ com r fatores absolutamente irredutíveis distintos e $mdc(f, \frac{\partial f}{\partial x}) = 1$. Seja S um subconjunto finito de F e $\{g_1, ..., g_r\}$ uma base de G' sobre F. Escolha $a_i \in S$ de forma uniformemente aleatória e independente, $1 \leq i \leq r$, e seja $g = \sum_{i=1}^{r} a_i g_i$. Então, a probabilidade de que se obtenha uma fatoração completa de f sobre $\bar{F}$ ou, equivalentemente, que $E_g(x)$ seja separável, é de pelo menos $1 - r(r-1)/(2|S|)$*

Demonstração

Do corolário (3.1.12) sabemos que existe uma matriz $A \in \bar{F}^{r \times r}$ tal que

$$\begin{bmatrix} g_1 \\ . \\ g_r \end{bmatrix} = A \begin{bmatrix} E_1 \\ . \\ E_r \end{bmatrix}.$$

de forma que

$$g = \sum_{i=1}^{r} a_i E_i = \begin{bmatrix} a_1 & . & a_r \end{bmatrix} A \begin{bmatrix} E_1 \\ . \\ E_r \end{bmatrix}.$$

Seja $[\lambda_1 \quad . \quad \lambda_r] = [a_1 \quad . \quad a_r]A$. Nesse caso, $g = \sum_{i=1}^{r} \lambda_i E_i$ e $E_g(x) = \prod_{i=1}^{t}(x - \lambda_i)$. Também pelo corolário (3.1.12), E_g fornece uma fatoração completa se, e somente se, E_g não possui raízes repetidas em $\bar{F}$, isto é, se todos os λ_i's forem distintos. Recaímos no lema acima, de onde vem que a propriedade de isso acontecer é de pelo menos $1 - \frac{r(r-1)}{2|S|}$. $\square$

Já que $r \leq m$, a probabilidade de que o elemento g escolhido resulte em um polinômio em uma variável E_g separável é de pelo menos $1/2$ se $|S| > m^2$. Também é claro que, desde que o corpo F tenha elementos suficientes, o conjunto S pode ser aumentado para que a probabilidade de um polinômio separável ser encontrado seja arbitrariamente próxima de 1.

Nesse momento, estamos em condições de enunciar o algoritmo de Gao para fatoração de polinômios em duas variáveis sobre um corpo F com característica zero ou superior a $(2m-1)n$ elementos.

Algoritmo 3.2.5. *Algoritmo de Gao*

Entrada: *Um polinômio $f \in F[x,y]$, satisfazendo $mdc(f, \frac{\partial f}{\partial x}) = 1$, onde (m,n) é o grau de f em x e y, respectivamente, e F é um corpo de característica zero ou superior a $(2m-1)n$. Um subconjunto $S \subset F$ de cardinalidade mn.*

Saída: *Duas listas: RL para a lista de todos os fatores racionais irredutíveis de f. AL para a lista dos fatores absolutamente irredutíveis de f, dois a dois não algebricamente conjugados sobre F.*

1. $RL \leftarrow \emptyset, \;\; AL \leftarrow \emptyset$
2. *construa o sistema linear de Gao e encontre uma base G para o seu espaço nulo sobre F*
   se $r = 1$, então devolva $RL = \{f\}$ e $AL = \{[f,x]\}$
3. *escolha $a_i \in S$ de forma uniformemente aleatória e independente, $1 \leq i \leq r$*
   $g \leftarrow \sum_{i=1}^{r} a_i g_i$
4. *calcule $E_g(x)$ como no corolário (3.1.12). Se E_g não for separável, vá para* 3
5. *fatore $E_g(x)$ em $F[x]$*
   $f_0 \leftarrow f$, o polinômio ainda a ser fatorado
6. *para cada fator simples $\phi(x)$ de $E_g(x)$ faça*
   calcule $f_1 = mdc(f, g - \lambda \frac{\partial f}{\partial x})$ em $L[x,y]$, onde $L = F[t]/(\phi(t))$ e
   λ é a classe de congruência de t, isto é, uma raiz de $\phi(t)$ em L
   calcule $h_1 = mdc(f_0, \frac{\partial f}{\partial x}^{\gamma} \phi(g/\frac{\partial f}{\partial x})) \in F[x,y]$, onde $\gamma = grau\ \phi(x)$
   $RL \leftarrow RL \cup \{f_1\}, \;\; AL \leftarrow AL \cup \{[h_1, \phi]\}$
   $f_0 \leftarrow f_0/h_1$
8. *devolva as listas RL e AL*

Os próximos teoremas se preocuparão com a validade e a análise de complexidade para esse algoritmo.

Teorema 3.2.6. *O algoritmo de Gao calcula corretamente a fatoração racional* $f = h_1...h_s$, *onde* $h_i \in F[x,y]$ *são distintos e irredutíveis e uma lista* $f_1, ..., f_s \in \bar{F}[x,y]$ *de fatores absolutamente irredutíveis de* f *tais que* f_i *divide* h_i, $1 \leq i \leq s$. *Se o polinômio* f *também for primitivo com respeito à variável* x, *então se espera realizar os passos* 3 *e* 4 *apenas duas vezes.*

Demonstração

Praticamente todo o trabalho já foi feito em resultados anteriores. A única afirmação que ainda devemos verificar é aquela sobre o número de iterações esperadas para os passos 3 e 4. Mas, com a suposição adicional de que f é primitivo com respeito a x (já, sabíamos disso com respeito a y, pois $mdc(f, \frac{\partial f}{\partial x}) = 1$), o número r de fatores absolutamente irredutíveis é limitado por $min\{m,n\}$, logo $Prob(E_g\ separ\acute{a}vel) \geq 1 - r(r-1)/2|S| = 1 - r(r-1)/2mn > 1/2$. □

Teorema 3.2.7. *Se* F *é um corpo finito* F_q *de característica superior a* $6mn$, *então se espera que o algoritmo de Gao termine utilizando* $O(r(mn)^2 log^2(mn) + r^2 log(q))$ *operações em* F_q, *onde* r *é o número de fatores absolutamente irredutíveis de* f.

Demonstração

O maior custo computacional do algoritmo de Gao está no segundo passo, onde um sistema linear grande deve ser resolvido. De fato, o enunciado do problema de Gao associado a f (3.1) implica que g e h têm $m(n+1)$ e $(m+1)n$ coeficientes, respectivamente. Além disso, o sistema conta com $4mn$ equações. Portanto, temos de encontrar o espaço nulo de um sistema de $O(mn)$ equações com $O(mn)$ indeterminadas. Utilizando uma técnica que se denomina caixa preta, isso pode ser feito em $O(rmn)$ produtos entre matrizes e vetores, conforme o trabalho de E. Kaltofen e B. Trager [Kaltofen e Trager, 1990]. Pela equação (3.2), cada produto

entre vetor e matriz pode ser calculado por três multiplicações de polinômios em $F_q[x, y]$ de grau limitado por (m, n), que requerem $O(mnlog^2(mn))$ operações em F_q. Logo, o passo 2 exige $O(r(mn)^2log^2(mn))$ operações em F_q.

O passo 3 é trivial e não afetará a complexidade do algoritmo. Para o passo 4, primeiro calcularemos os restos de $gg_i, g_i\frac{\partial f}{\partial x}$ módulo f (sob alguma ordem de termos, por exemplo, a ordem $DegLex$). Cada um desses restos tem no máximo $4mn$ termos, logo corresponde a um vetor de comprimento $4mn$. Mas encontrar a matriz $A = (a_{ij})$ do corolário (3.1.12) é equivalente a expressar r vetores de comprimento $4mn$ como combinações lineares de r vetores dados de algum comprimento pré-determinado. Isso pode ser feito por eliminação Gaussiana com um custo de $O(r^2mn)$ operações em F_q. Já o polinômio característico $det(Ix - A)$ pode ser calculado em $O(r^3) = O(rmn)$ operações em F_q. Portanto, o passo 4, utiliza $O(r^2mn)$ operações em F_q. Espera-se que ele seja realizado no máximo duas vezes. No passo 5, devemos fatorar E_g, que é um polinômio em uma variável de grau r, o que exige $O(r^3 + r^2log\ q) = O(rmn + r^2log\ q)$ operações em F_q. No passo 6, f_1 pode ser calculado em $O(mnlog^2(mn))$ operações em $L = F_q[t]/(\phi(t))$ e portanto $O(\gamma^2mnlog^2(\gamma^2mn)) = O((mn)^2log^2(mn))$ operações em F_q, lembrando que γ é o grau do fator ϕ. O polinômio h_1, por sua vez, é o máximo divisor comum de dois polinômios com graus limitados por (m, n) e $(\gamma m, \gamma n)$, respectivamente, e também pode ser obtido com $O(\gamma^2mnlog^2(\gamma^2mn)) = O((mn)^2log^2(mn))$ operações sobre F_q. Logo, o custo para obter todos os fatores f_1, h_1 é limitado por $O(r(mn)^2log^2(mn))$.

O custo total do algoritmo é

$$O(r(mn)^2log^2(mn) + r^2mn + rmn + r^2log\ q + r(mn)^2log^2(mn)) =$$
$$O(r(mn)^2log^2(mn) + r^2log\ q)$$

operações em F_q. □

A análise da complexidade do algoritmo sobre os números complexos deve ser feita com mais cuidado e não será mencionada nesse trabalho. S. Gao comenta algumas dificuldades envolvidas em [Gao, 2003].

Desde a descoberta de seu algoritmo, S. Gao e diversos colaboradores estabeleceram melhorias, como a considerável redução, para polinômios esparsos, do número de equações no sistema induzido pela equação diferencial associada ao problema [Gao e Rodrigues, 2003], ou forneceram novas aplicações, como a incorporação de métodos numéricos para o desenvolvimento de um método eficiente para fatoração aproximada de polinômios [Gao et al.,].

3.3 Aplicações e Exemplos

A seção que aqui se inicia trata de aplicações adicionais ao que já foi feito, bem como de exemplos que ilustram restrições em nossos algoritmos ou mesmo dificuldades que ainda precisam ser transpostas.

As aplicações a que nos referimos dizem respeito à fatoração de polinômios em fatores racionais. O resultado crucial para estabelecê-las vem da teoria que vimos na primeira seção e relaciona o que denominamos teste $1-dimensional$ com a fatoração de f em elementos irredutíveis racionais. Analisando esse caso com maior profundidade do que já foi feito na proposição (3.1.5), estabeleceremos o seguinte resultado:

Teorema 3.3.1. *Fatores irredutíveis racionais*

Sejam F um corpo e $f \in F[x,y]$ de grau (m,n). Suponhamos também que $mdc(f, \frac{\partial f}{\partial x}) = 1$ e que f tenha r fatores irredutíveis distintos em $\bar{F}[x,y]$, digamos $f = f_1 f_2 ... f_r$. Seja G'' o subespaço vetorial de G' gerado pelos elementos $g \in G$ satisfazendo o teste $1-dimensional$, isto é, tais que $g^2 \equiv ag\frac{\partial f}{\partial x}$ mod f, para certo $a \in F$.

Então, a dimensão de G'' é igual ao número de fatores irredutíveis de f sobre $F[x,y]$.

Para provar esse teorema, recorreremos a um lema técnico.

Lema 3.3.2. *Sejam $f, g \in \bar{F}[x,y]$ polinômios separáveis tais que $fg \in F[x,y]$ é livre de quadrados e $\frac{\partial f}{\partial x}g \in F[x,y]$, com $\frac{\partial f}{\partial x} \neq 0$. Então, existe $\alpha \in \bar{F}$ tal que $\alpha g \in F[x,y]$.*

Demonstração

Sejam $f_1, f_2, ..., f_r,\ g_1, g_2, ..., g_s$ os fatores irredutíveis de f e g sobre $\bar{F}[x,y]$, respectivamente. Suponha, por absurdo, que $\alpha g \notin F[x,y]$, $\forall \alpha \in \bar{F}$. Portanto, existe um fator irredutível $\hat{f}$ de fg sobre $F[x,y]$ escrito como produto de f_i's e g_j's, mas que não pode ser escrito como um produto apenas de f_i's ou de g_j's.

Sejam $i_0 \in \{1, 2, ..., r\}$, $j_0 \in \{1, 2, ..., r\}$ tais que f_{i_0}, g_{j_0} são elementos na expansão de $\hat{f}$ satisfazendo essa propriedade.

Mas, como g_{j_0} divide o polinômio irredutível $\hat{f}$, $\hat{f}$ também dividirá $\frac{\partial f}{\partial x}g$, que é um polinômio não nulo. Isso é absurdo, pois f_{i_0} não divide $\frac{\partial f}{\partial x}g$, visto que f é separável e $g_k \neq f_{i_0}$, $\forall\ k$, pelo fato de fg ser livre de quadrados. □

Tendo esse resultado em mãos, procederemos com a demonstração do teorema.

Demonstração do teorema

Seja $g \in G$ tal que $g(g - a\frac{\partial f}{\partial x}) \equiv 0\ mod\ f$, para certo $a \in F$. Pela demonstração do teorema (3.1.5), se um polinômio $\hat{g}$ é solução do teste $s-dimensional$, então $\hat{g} = \sum_{i=1}^{s}(\alpha_i \sum_{j \in P_i} E_j)$, onde α_i são as raízes em $\bar{F}$ do polinômio característico da matriz A e $P_1, ..., P_s$ são subconjuntos do conjunto de índices $\{1, 2, ..., r\}$ associado aos fatores absolutamente irredutíveis de f. Em nosso caso, $s = 1$, logo todo g satisfazendo o teste $1 - dimensional$ tem a forma

$$g = a \sum_{i \in \Lambda} E_i,$$

para certo $\Lambda \subseteq \{1, 2, ..., r\}$. É fácil ver que, reciprocamente, todo g com o formato acima satisfaz o teste $1-dimensional$. Conseqüentemente, G'' é o subespaço vetorial de G' gerado pelos elementos $g = a \sum_{i \in \Lambda} E_i$, onde $a \in F$ e $\Lambda \subseteq \{1, 2, ..., r\}$.

Seja $\hat{f}$ um fator irredutível racional de f e suponha, sem perda de generalidade, que $\hat{f} = f_1 f_2 ... f_s$. Definimos

$$\hat{E} = E_1 + ... + E_s = \sum_{i=1}^{s} \frac{f}{f_i}\frac{\partial f_i}{\partial x} = (f_{s+1}...f_r)\sum_{i=1}^{s} \frac{\hat{f}}{f_i}\frac{\partial f_i}{\partial x} = f_{s+1}...f_r\frac{\partial \hat{f}}{\partial x} \in F[x,y].$$

Portanto, associado a cada fator irredutível $\hat{f}$ de f está um elemento $\hat{E}$ pertencente a G'' por nossa discussão prévia. Pela independência linear dos E_i's, elementos associados a fatores racionais distintos de f são linearmente independentes.

Seja agora $g \in G$ satisfazendo $g^2 \equiv agf_x \ mod \ f$, para certo $a \in F$. Então, existem índices em $\{1, 2, .., r\}$, digamos $\{1, 2, .., s\}$ tais que $g = a\sum_{i=1}^{s} E_i$.

Seja $\hat{f} = f_1...f_s$. Por cálculos simples, obtém-se $g = af_{s+1}...f_r\frac{\partial \hat{f}}{\partial x}$.

Segue que $\hat{f}$ e $af_{s+1}...f_r$ são polinômios separáveis tais que $af_{s+1}...f_r\hat{f} = af$ e $af_{s+1}...f_r\frac{\partial \hat{f}}{\partial x} = ag$ estão em $F[x,y]$, sendo o primeiro deles livre de quadrados e o segundo não nulo. Pelo lema, existe $\alpha \in F$ tal que $\alpha\hat{f} \in F[x,y]$. Por simplicidade, digamos que $\hat{f} \in F[x,y]$. É claro então que g é a soma dos elementos associados aos fatores irredutíveis de $\hat{f}$ obtidos na prova do outro sentido dessa mesma proposição.

Estabeleceu-se a igualdade entre a dimensão de G'' e o número de fatores irredutíveis de f. □

Um corolário imediato desse teorema, que nos fornece um teste de irredutibilidade para polinômios em $F[x,y]$, é:

Corolário 3.3.3. *Teste de irredutibilidade*

Um polinômio $f \in F[x,y]$ é irredutível se, e somente se, a dimensão do espaço G'' associado a ele é igual a um.

Cálculos análogos aos feitos em resultados anteriores resultam em outro corolário:

Corolário 3.3.4. *Recuperação de fatores irredutíveis racionais*

Sejam F um corpo e $f \in F[x,y]$ de grau (m,n). Suponhamos também que $mdc(f, f_x) = 1$ e que $\{g_1, ..., g_s\}$ é uma base para o espaço vetorial G'' definido acima. Então, para cada $k \in \{1, 2, ..., s\}$, existe uma única matriz $A_k = (a_{ij}^k) \in F^{s\times s}$ tal que

$$g_k g_i \equiv \sum_{j=1}^{s} a_{ij}^k g_j \frac{\partial f}{\partial x} \ mod \ f.$$

Se definirmos $E_{g_k}(x) = det(I_{s\times s}x - A_k)$, o polinômio característico de A_k, a fatoração de E_{g_k} em elementos irredutíveis $\phi(x)$ em $F[x]$ resultará numa fatoração de f em fatores próprios dados por $mdc(f, \frac{\partial f}{\partial x}^t \phi(g_k/\frac{\partial f}{\partial x}))$ em $F[x,y]$. Combinando as fatorações geradas por todos os g_k's, obtemos a fatoração irredutível racional de f.

Em outras palavras, esse resultado estabelece que, se utilizarmos G'' ao invés de G', as mesmas idéias empregadas no algoritmo (3.1.14) resultam na fatoração de f em elementos racionais. Sua demonstração se baseia nas provas dos corolários (3.1.11) e (3.1.12) e da proposição (3.1.13).

Em muitas oportunidades, quando temos um polinômio $f = gh \in F[x,y]$, onde $g, h \in F[x,y]$ não são constantes, a dimensão do espaço vetorial G de soluções para o problema de Gao associado a f é maior do que a soma das dimensões dos espaços análogos associados a g e h. Além disso, a cota no número de testes $s - dimensionais$ que devem ser realizados para obter G' pelo algoritmo (3.1.14) é dada pelo grau em x do polinômio a ser fatorado. Certamente, uma cota mais conveniente é o máximo dos graus em x dos fatores irredutíveis do polinômio em $F[x,y]$. Isso justifica a seguinte variante do algoritmo de Gao estendido:

Algoritmo 3.3.5.

Entrada: *Um corpo F, $f \in F[x,y]$, satisfazendo $mdc(f, \frac{\partial f}{\partial x}) = 1$, onde (m,n) é o grau de f em x e y, respectivamente.*

Saída: *Duas listas: RL para a lista de todos os fatores racionais irredutíveis de f. AL para a lista dos fatores absolutamente irredutíveis de f, dois a dois não algebricamente conjugados sobre F.*

1. $C \leftarrow \emptyset$
2. *construa o sistema linear de Gao e encontre uma base G para o seu espaço nulo sobre F*
3. *determine uma base $\{g_1, ..., g_s\}$ para o subespaço vetorial G'' de G pelo teste $1-$dimensional*
   se $s = 1$, então devolva $RL = \{f\}$ e $AL = \{[f, x]\}$
   calcule o conjunto de fatores irredutíveis $RL = \{\hat{f}_1, ..., \hat{f}_s\}$ de f pelo corolário (3.3.4) e pelo algoritmo (3.1.9)
4. *para $i = 1, 2, ..., s$*
5. *utilize o algoritmo (3.1.14) para obter os conjuntos AL_i de fatores absolutamente irredutíveis de $\hat{f}_i$*
6. $AL = \bigcup_{i=1}^{s} AL_i$
7. *devolva as listas RL e AL*

Apliquemos esse algoritmo a nosso tradicional exemplo:

Exemplo 3.3.6. *Tratávamos da fatoração do polinômio*

$$f(x,y) = x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1$$

em $F_2[x,y]$. Assim como mencionado anteriormente, $B = \{1 + y + y^2 + x^3y^4 + x^3y^5, xy^4 + xy^5 + x^2y^3 + x^3y^2 + x^4y^2, y^3 + y^4 + xy^2 + x^2y + x^3y, x^3y^2 + x^3y^3 + x^4y^2, xy^2 + xy^3 + x^2y + x^3y, y + y^2 + xy, x^2y^3 + x^2y^4 + x^3y^2 + x^4y^2, x^2y + x^2y^2 + x^3y, 1 + y + y^2 + x^4y^4\}$

é uma base para G *e* $B_1 = \{x^4y^4+y^2+y+1, xy+y^2+y\}$ *é uma base para as soluções do teste* $1-$*dimensional, ou seja, uma base para* G''.

A matriz $A_1 \in F_2^{2\times 2}$ *análoga à do corolário (3.1.12) para* $g = g_1 = x^4y^4 + y^2 + y + 1$ *é*

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

e nos dá o polinômio $E_{g_1}(x) = (x+1)^2$, *que por sua vez origina o conjunto* $RL_1 = \{x^5y^4 + x^4y^5 + x^4y^4 + x^2y + xy^2 + xy + x + y + 1\}$, *que não nos fornece qualquer informação. Para* $g = g_2$, *porém, obtém-se a matriz*

$$A_2 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

que leva ao polinômio $E_{g_2}(x) = x(x+1)$, *do qual vem a fatoração* $RL_2 = \{x+y+1, x^4y^4 + xy + 1\}$, *que vem a ser fatoração de* f *em fatores irredutíveis racionais. Observemos que a justificativa para isso é o fato de uma base de* G'' *ser um conjunto de separação para fatores irredutíveis racionais, assim como* G' *o é para fatores irredutíveis absolutos.*

Agora, aplicamos o algoritmo (3.1.14) para cada um dos fatores irredutíveis de f *para encontrar a fatoração absolutamente irredutível. Para o primeiro polinômio, o espaço solução* G *do problema de Gao associado tem dimensão unitária, logo* $x+y+1$ *já é absolutamente irredutível. No caso* $f = x^4y^4+xy+1$, *uma base para* G *é* $B = \{xy^2, x^2y, x^2y^3, y^3, x^3y^2, x^3y^4, xy^4, y\}$ *e, aplicando testes* $s-$*dimensionais até* $s = 4$, *vem que* $B' = \{xy^2, y, x^2y^3, x^3y^4\}$ *é uma base para* G'. *Fazendo cálculos análogos aos do último exemplo, obtemos uma fatoração para cada elemento* g *da base de* G' *via seu polinômio associado* E_g *e ,assim como no último exemplo, a fatoração completa*

$$x^4y^4 + xy + 1 = (xy + \lambda)(xy + \lambda^2)(xy + \lambda + 1)(xy + \lambda^2 + 1),$$

onde λ *é uma raiz de* x^4+x+1, *será obtida sem que haja necessidade de recombinação de fatores.*

Mesmo que essa versão para o algoritmo de Gao modificado seja melhor que a anterior em geral, não há diferença entre as duas nos casos em que f já é irredutível sobre $F[x, y]$ e G é um espaço vetorial de dimensão grande. Portanto, para que uma versão desse algoritmo possa ser mais eficaz em diversas situações práticas, deveremos encontrar um método mais eficiente para obter G' a partir de G. O seguinte exemplo ilustra que essa tarefa não parece ser fácil:

Exemplo 3.3.7. *Seja o polinômio $f = x^7y^4 + y^6 + xy^4 + x^2 + x$, que sabemos ser absolutamente irredutível em $F_2[x, y]$. Ao se procurar uma base para o espaço vetorial G das soluções do problema de Gao, deparamos com um conjunto de 28 elementos. Já é um trabalho árduo encontrar uma solução para o teste $1-$dimensional nessas condições, e aplicar cada um dos testes $s-$dimensionais, para $s = 1, 2, ..., 7$ é bastante trabalhoso. De fato, dos 28 monômios que integram a base de G, apenas três contribuem na formação do polinômio $g = x^6y^4 + y^4 + 1$, que constitui a base de G'.*

Mas nem tudo são más notícias: na prática, é bastante comum que o espaço solução G do problema de Gao coincida com G', o que evita que G' tenha de ser recuperado: aliás, isso pode ser testado antes do cálculo de G', bastando para isso verificar se existem matrizes A da forma do corolário (3.1.12) para os elementos de G. Por exemplo, pode-se mostrar por um método geométrico baseado em figuras convexas denominadas polytopes de Newton que o polinômio f definido acima é absolutamente irredutível em $F[x, y]$ para qualquer corpo F (vide o trabalho [Gao, 2001], também de S. Gao para maiores informações). Mas, para todos os corpos finitos de característica $p > 2$, resulta que G tem dimensão um e não precisamos calcular G', embora a cota na característica fornecida por Gao só garanta isso para primos maiores do que $(2m - 1)n = (2 \cdot 7 - 1)6 = 78$.

Para ilustrar que esse comportamento não é isolado, incluímos nesse momento uma tabela formada por polinômios bivariados sobre o corpo F, a respectiva cota de Gao para a característica de F tal que $G' = G$ e os primos inferiores a

essa cota para que $G' \neq G$, com o dado adicional da diferença entre as dimensões dos espaços vetoriais G e G' obtidos.

Polinômio	**Cota de Gao**	**Primos para que $G' \neq G$**
$(x-y)(x+y)(x+y+1)(x^3-y+7)$	44	$[2, mdc], [3, mdc]$
$(x^7-y^5)(x+y^2)$	105	$[2,19], [3,17], [5,13], [7, mdc]$ $[11,2], [13,2], [23,2]$
$(x^7-y^5+1)(x+y^2)$	105	$[2,8], [3,3], [5,13], [7, mdc]$
$(x^3-2xy)(xy^2+1)$	21	$[2, mdc], [5,1]$
$(x^7-9y^5+xy)(xy^2+xy+1)$	105	$[2,5], [3, mdc], [5,1]$
$(x^2-y)(x^2+y)(xy^3+4)$	45	$[2, mdc], [3,3], [7,3]$

4 CONCLUSÃO

Na presente dissertação, retratamos o problema de fatoração de polinômios em duas variáveis com coeficientes em um corpo. Nossas contribuições à generalização do algoritmo de Gao para fatoração de polinômios em duas variáveis exercem um papel de destaque. Em segundo plano, encontra-se um apanhado histórico da fatoração de polinômios em duas variáveis.

No que se refere a esse último aspecto, fizemos no capítulo 2 uma descrição dos sucessivos avanços em técnicas de fatoração que desembocaram em um algoritmo em tempo polinomial para esse problema, um dos grandes sucessos da Álgebra Computacional nos anos 80. Ferramentas como computação por imagens homomórficas, levantamento de fatorações e redução de base em reticulados foram introduzidas naturalmente nesse contexto. Além disso, o apêndice 1 ressaltou a relevância de nossa opção pelo caso específico de duas variáveis, já que apresenta um método de redução para que polinômios em mais variáveis recaiam nele.

A contribuição principal desse trabalho consistiu, contudo, no estudo do algoritmo de Gao para fatoração de polinômios em duas variáveis. Dado um polinômio $f \in F[x, y]$, obtivemos êxito em desenvolver uma teoria mais geral para o espaço vetorial de soluções polinomiais do problema de Gao associado a f, isto é, o espaço vetorial das soluções polinomiais da equação diferencial que motiva o algoritmo de Gao. De fato, determinamos um subespaço vetorial cuja dimensão coincide com o número de fatores absolutamente irredutíveis de f e a partir do qual os fatores irredutíveis racionais e absolutos de f podem ser recuperados. Principalmente, elaboramos um algoritmo que obtém esse subespaço a partir do espaço original para corpos finitos, e que induz uma extensão do algoritmo de Gao. Além disso, analisando um caso particular do teste que serve de embasamento para nosso algoritmo, identificamos um segundo subespaço vetorial com dimensão igual ao número de fatores irredutíveis racionais de f e que por sua vez possibilita a recuperação desses elementos.

Um dos problemas de nossa generalização é o custo computacional exponencial do método que desenvolvemos para determinar o subespaço vetorial necessário. Portanto, uma pesquisa com o objetivo de encontrar um modo mais eficaz de determinar esse subespaço será de grande valia para transformar nossa extensão em um algoritmo mais competitivo. À primeira vista, essa tarefa pode ser difícil, mas, se obtivermos pelo menos um modo eficiente de calcular o subespaço vetorial menor que fornece os fatores irredutíveis racionais do polinômio, já teremos um bom algoritmo para determinar os fatores irredutíveis racionais de f. Isso implicaria, por exemplo, que um teste para determinar o subespaço maior poderia se concentrar unicamente no caso de polinômios irredutíveis em $F[x, y]$. Outra sugestão para pesquisas futuras que foi mencionada em nosso trabalho, embora não tenha sido estudada com maiores detalhes, é a procura de uma cota melhor para a característica a partir da qual garantimos a igualdade entre o subespaço que procuramos e o próprio espaço solução do problema de Gao. Observamos no início do trabalho que mesmo S. Gao acredita que essa cota possa ser melhorada e vimos no capítulo 3 como ela proveio de um argumento peculiar.

Se essas dificuldades forem vencidas, uma versão estendida do algoritmo de Gao será certamente uma alternativa atraente para fatorar polinômios em duas variáveis sobre uma ampla classe de corpos.

BIBLIOGRAFIA

[Berlekamp, 1970] Berlekamp, E. R. (1970). Factoring polynomials over large finite fields. *Mathematics of Computation*, 24:713–735.

[C. Bajaj e Warren, 1993] C. Bajaj, J. Canny, T. G. e Warren, J. (1993). Factoring rational polynomials over the complex numbers. *SIAM Journal of Computation*, 22:318–331.

[Díaz e Kaltofen, 1998] Díaz, A. e Kaltofen, E. (1998). *FOXBOX: A system for manipulating symbolic objects in black box representation*, pages 30–37. ACM Press.

[Gao, 2001] Gao, S. (2001). Absolute irreducibility of polynomials via newton polytopes. *Journal of Algebra*, 237:501–520.

[Gao, 2003] Gao, S. (2003). Factoring multivariate polynomials via partial differential equations. *Mathematics of Computation*, 72:801–822.

[Gao et al.,] Gao, S., Kaltofen, E., May, J. P., Yang, Z., e Zhi, L. Approximate factorization of multivariate polynomials via differential equations. *ISSAC 2004 - to appear*.

[Gao e Rodrigues, 2003] Gao, S. e Rodrigues, V. M. (2003). Irreducibility of polynomials modulo p via newton polytopes. *Journal of Number Theory*, 101:32–47.

[Garcia e Lequain, 2002] Garcia, A. e Lequain, Y. (2002). *Elementos de Álgebra*. Editora do IMPA.

[Hartshorne, 1977] Hartshorne, R. (1977). *Algebraic Geometry*. Springer Verlag.

[Hensel, 1918] Hensel, K. (1918). Eine neue theorie der algebraischen zahlen. *Mathematische Zeitschrift*, 2:433–452.

[Hilbert, 1892] Hilbert, D. (1892). Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficientes. *Journal für die Reine und Angewandte Mathematik*, 110:104–129.

[Jacobson, 1964] Jacobson, N. (1964). *Lectures in Abstract Algebra*. Van Nostrand.

[Kaltofen, 1985] Kaltofen, E. (1985). Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. *SIAM Journal on Computing*, 14(2):469–489.

[Kaltofen, 1989] Kaltofen, E. (1989). *Factorization of polynomials given by straight-line programs*, pages 375–412. JAI Press.

[Kaltofen, 1995] Kaltofen, E. (1995). Effective noether irreducibility forms and applications. *Journal of Computer and System Sciences*, 50:274–295.

[Kaltofen et al., 1983] Kaltofen, E., Musser, D. R., e Saunders, B. D. (1983). A generalized class of polynomials that are hard to factor. *SIAM Journal on Computing*, 12:473–483.

[Kaltofen e Trager, 1990] Kaltofen, E. e Trager, B. (1990). Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *Journal of Symbolic Computation*, 9:301–320.

[Knuth, 1969] Knuth, D. E. (1969). *The Art of Computer Programming*. Addison-Wesley Publishing Company.

[Landau, 1985] Landau, S. (1985). Factoring polynomials over finite fields. *SIAM Journal on Computing*, 14:185–195.

[Lang, 1961] Lang, S. (1961). *Diophantine Geometry*. John Wiley and Sons.

[Lang, 1965] Lang, S. (1965). *Algebra*. Addison-Wesley Publishing Company.

[Lenstra et al., 1982] Lenstra, A. K., Lenstra, H. W., e Lovász, L. (1982). Factoring multivariate polynomials with rational coefficients. *Mathematische Annalen*, 161:515–534.

[Minkowski, 1910] Minkowski, H. (1910). *Geometrie der Zahlen*. B. G. Teubner.

[Mumford, 1976] Mumford, D. (1976). *Algebraic Geometry I: Complex Projective Varieties*. Springer Verlag.

[Niederreiter, 1993] Niederreiter, H. (1993). A new efficient factorization algorithm for polynomials over small finite fields. *Appl. Alg. Eng. Comm. Comp.*, 4:81–87.

[Ruppert, 1999] Ruppert, W. M. (1999). Reducibility of polynomials $f(x, y)$ modulo p. *Journal of Number Theory*, 77:62–70.

[von zur Gathen, 1984] von zur Gathen, J. (1984). Hensel and newton methods in valuation rings. *Mathematics of Computation*, 42:637–661.

[von zur Gathen, 1985] von zur Gathen, J. (1985). Irreducibility of multivariate polynomials. *Journal of Computer and System Sciences*, 31:225–264.

[von zur Gathen e Gerhard, 1999] von zur Gathen, J. e Gerhard, J. (1999). *Modern Computer Algebra*. Cambridge University Press.

[von zur Gathen e Kaltofen, 1985] von zur Gathen, J. e Kaltofen, E. (1985). Factoring sparse multivariate polynomials. *Journal of Computer and System Sciences*, 31(2):265–287.

[Zassenhaus, 1969] Zassenhaus, H. (1969). On hensel factorization i. *Journal of Number Theory*, 1:291–311.

APÊNDICE A REDUÇÃO DA FATORAÇÃO EM VÁRIAS VARIÁVEIS A DUAS VARIÁVEIS

Esse apêndice enfatizará a relevância do presente trabalho ao mostrar como a fatoração de polinômios em muitas variáveis pode ser reduzida à fatoração de polinômios em apenas duas variáveis. Isso é feito a partir de uma versão eficiente do teorema de irredutibilidade de Hilbert, ou teorema de Bertini.

A versão original de Hilbert [Hilbert, 1892], publicada em 1892, enuncia que um polinômio $f \in \mathbb{Q}[x, y]$ em muitos casos origina um polinômio irredutível $f(x, a) \in \mathbb{Q}[x]$ quando a variável y for substituída por um número inteiro a. Segue uma versão retirada de [Lang, 1961]:

Teorema A.1. *Irredutibilidade de Hilbert*

Seja $f \in \mathbb{Q}[x, y]$ um polinômio irredutível. O subconjunto de Hilbert de $\mathbb{Q}$ associado a f, isto é, o conjunto de elementos $a \in \mathbb{Q}$ que quando substituídos na variável y geram um polinômio irredutível $f(x, a)$ em $\mathbb{Q}[x]$, é denso em $\mathbb{Q}$ para sua topologia usual e qualquer topologia p-ádica.

Esse fato não é verdadeiro para polinômios sobre corpos finitos ou mesmo sobre os números complexos e, mesmo para os números racionais, as muitas generalizações e melhoramentos da versão original não foram suficientemente fortes até o momento para que delas se derivasse um algoritmo probabilístico eficiente.

Porém, a situação será diferente quando aceitarmos uma variável a mais e realizarmos substituições da forma $ax_1 + bx_2 + c$, onde a, b, c são escolhidos aleatoriamente de um subconjunto finito (suficientemente numeroso) do corpo base. Nesse caso, para polinômios irredutíveis em $F[x_1, ..., x_n]$, o polinômio obtido por substituição em $F[x_1, x_2]$ será quase sempre irredutível. Isso motiva que desenvolvamos um procedimento com a seguinte estrutura: um polinômio arbitrário será transformado

em um polinômio em duas variáveis por uma aplicação de substituição e o polinômio que resulta é então fatorado utilizando um método para duas variáveis. Finalmente, aplicam-se métodos de interpolação para recuperar os fatores nas várias variáveis originais. O papel da versão efetiva do teorema de irredutibilidade de Hilbert é garantir que, com alta probabilidade, não devemos nos preocupar com a "quebra" de fatores após a substituição ou, melhor dizendo, o número de fatores irredutíveis antes e após a substituição permanece inalterado. Observemos que esse não foi o caso quando tratamos de algoritmos modulares para duas variáveis. Nessa ocasião, tanto levamos em conta a possibilidade de que fatores irredutíveis em $F[x, y]$ pudessem perder esse status módulo p, que tivemos que desenvolver toda uma teoria baseada em redução de base em reticulados para recompor os fatores originais. Infelizmente, um procedimento similar não teria êxito em tempo polinomial quando tratamos com polinômios a mais variáveis, por motivos que veremos adiante.

Tratemos então do teorema de Bertini. Esse resultado estabelece, entre outras coisas, que a interseção de um conjunto algébrico irredutível com um plano genérico é irredutível (uma curva irredutível). Mais precisamente,

Teorema A.2. *Bertini*

(*i*) *Seja X uma variedade projetiva não singular sobre um corpo K algebricamente fechado de característica zero. Seja Υ um sistema linear sem pontos base. Então, quase todo elemento de Υ, considerado como sub-esquema fechado de X, é não-singular (mas pode ser redutível).*

(*ii*) *Seja X uma variedade projetiva normal sobre um corpo algebricamente fechado K. Seja Υ um sistema linear de divisores efetivos de Cartier sem pontos base. Suponha também que, se $f : X \to P^n_K$ é o morfismo determinado por Υ, tem-se dim $f(X) \geq 2$. Então, os divisores em Υ são conexos e, portanto, quase todos são irredutíveis e não-singulares.*

O teorema foi enunciado em um contexto bastante geral e utiliza a terminologia da Geometria Algébrica, o que ilustra o arcabouço teórico que sustenta

essa teoria. Não discutiremos isso com profundidade, e leitores interessados podem se dirigir ao livro de R. Hartshorne [Hartshorne, 1977].

No nosso caso, um polinômio define uma hipersuperfície cujas componentes irredutíveis correspondem aos fatores absolutamente irredutíveis do polinômio. Se escolhermos um plano ao acaso e determinarmos sua intersecção com essa hipersuperfície, a questão que surge é com que probabilidade a intersecção do plano com cada uma das componentes irredutíveis da hipersuperfície permanece irredutível. Para objetivos algorítmicos, devemos dispor de uma cota para essa probabilidade, a saber, uma versão efetiva do teorema de irredutibilidade de Hilbert.

Sejamos precisos: escolhamos $f \in F[x_1, ..., x_n]$ com grau total d. Um plano em F^n pode ser parametrizado como

$$x_i = a_i x + b_i y + c_i, 1 \leq i \leq n,$$

para $a_i, b_i, c_i \in F$. A intersecção da hipersuperfície definida por f com o plano acima é uma curva em F^n isomorfa à curva plana definida pelo polinômio em duas variáveis

$$f_0 = f(a_1 x + b_1 x + c_1, ..., a_n x + b_n y + c_n) \in F[x, y]. \tag{A.1}$$

Isso nada mais é do que a substituição das variáveis de f que propusemos no início do capítulo. Suponha que os valores de $a_1, b_1, c_1, ..., a_n, b_n, c_n$ tenham sido escolhidos aleatoriamente em um subconjunto finito S de F. Queremos determinar a probabilidade de que todos os fatores irredutíveis de f se mantenham irredutíveis após a substituição. Para os números complexos, C. Bajaj et al [C. Bajaj e Warren, 1993] provaram, modificando a demonstração do teorema 4.17 do livro de Geometria Algébrica de Mumford [Mumford, 1976], que essa probabilidade é de pelo menos $1 - (d^4 - 2d^3 + d^2 + d + 1)/|S|$. Para corpos gerais, J. von zur Gathen demonstra em [von zur Gathen, 1985], empregando técnicas de teoria de eliminação, que a probabilidade é de pelo menos $1 - 9^{d^2}/|S|$. E. Kaltofen [Kaltofen, 1995] refinou essa cota para $1 - 2d^4/|S|$ em 1995, por meio de seu algoritmo de fatoração. O seguinte teorema traz ainda mais melhorias sobre corpos gerais e sua demonstração pode ser encontrada em S. Gao [Gao, 2003]:

Teorema A.3. *Sejam F um corpo e S um subconjunto finito de F. Seja $f \in F[x_1, ..., x_n]$ um polinômio de grau total d e f_0 definido a partir de f como em (A.1). Suponha que a característica de F seja zero ou superior a $2d^2$. Então, para escolhas aletórias de $a_i, b_i, c_i, 1 \leq i \leq n$ em S, todos os fatores absolutamente irredutíveis de f permanecem absolutamente irredutíveis como fatores de f_0 em $F[x, y]$ com probabilidade $1 - 2d^3/|S|$.*

Um algoritmo de fatoração de polinômios em duas variáveis, em conjunto com o teorema acima, estabelece um algoritmo probabilístico para polinômios em muitas variáveis. Para fatorar um polinômio $f \in F[x_1, ..., x_n]$ de grau total d, escolhem-se arbitrariamente valores $a_i, b_i, c_i, 1 \leq i \leq n$ em $S \subseteq F$ com $|F| \geq 4d^3$ e fatora-se $f_0 = f(a_1x + b_1x + c_1, ..., a_nx + b_ny + c_n)$ sobre $\bar{F}$. Pelo teorema acima, os fatores obtidos correspondem aos fatores de f avaliados nesses pontos com probabilidade de pelo menos $1/2$. Esse processo é repetido até que se acumule um número suficiente de fatorações e, em seguida, os verdadeiros fatores de f são recuperados por levantamento de Hensel e interpolação (para detalhes, vide [Kaltofen, 1985]).

Apesar de polinômios em várias variáveis não constituirem o objetivo principal desse trabalho, ainda concederemos espaço para comentários referentes à dificuldade de se manipular polinômios multivariados sob o ponto de vista de estrutura de dados.

Ao longo dessa dissertação, supomos, pelo menos implicitamente, que os polinômios em uma ou duas variáveis na entrada dos algoritmos estivessem armazenados no que chamamos de representação densa, isto é, um polinômio em $F_2[x_1, x_2, x_3]$ como $f = x_1^3 + x_1x_2^2 + x_3^3$, cujo grau total é igual a três, seria representado na forma $f = 1 \cdot x_1^3 + 0 \cdot x_1^2x_2 + 0 \cdot x_1^2x_3 + 0 \cdot x_1^2 + 1 \cdot x_1x_2^2 + 0 \cdot x_1x_3^2 + 0 \cdot x_1x_2x_3 + 0 \cdot x_1x_2 + 0 \cdot x_1x_3 + 0 \cdot x_1 + 0 \cdot x_2^3 + 0 \cdot x_2^2x_3 + 0 \cdot x_2^2 + 0 \cdot x_2x_3^2 + 0 \cdot x_2x_3 + 0 \cdot x_2 + 1 \cdot x_3^3 + 0 \cdot x_3^2 + 0 \cdot x_3 + 0 \cdot 1$. Adaptando as técnicas de fatoração em duas variáveis apresentadas no capítulo 1, poderíamos encontrar algoritmos que fatorassem polinômios multivariados em tempo polinomial *sobre o seu comprimento nessa representação.* E. Kaltofen [Kaltofen, 1985] indica como isso pode ser feito,

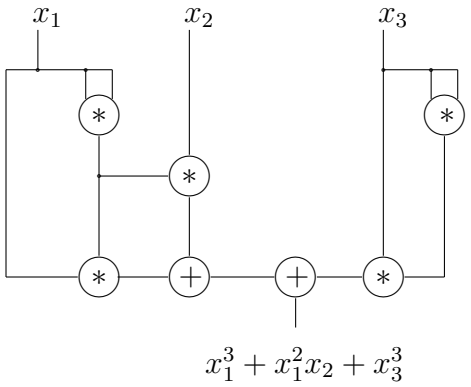
mas, evidentemente, somente esse resultado não seria satisfatório, pois, se d é o grau total do polinômio e n é o seu número de variáveis, apenas para armazená-lo seriam necessários

$$\alpha_{n,d} = \binom{n+d}{d} \tag{A.2}$$

termos. Haja vista o exemplo anterior, onde temos $\alpha_{3,3} = 20$ termos na representação, mesmo que o polinômio só possua três termos em sua representação usual, que denominaremos esparsa.

Infelizmente, nenhum algoritmo fatora polinômios multivariados em tempo polinomial sobre sua representação esparsa (para um algoritmo não polinomial, dirija-se por exemplo a [von zur Gathen e Kaltofen, 1985]). Há inclusive exemplos de famílias de polinômios tais que o comprimento da representação esparsa dos fatores (saída) é mais do que polinomial no comprimento do polinômio que se deseja fatorar nessa mesma representação. Isso sugere que representações ainda mais concisas devam ser procuradas. Por um lado, seria legítimo especular se isso não traria ainda mais discrepância entre os tamanhos de entrada e saída, mas representações inteligentes superarão isso.

Uma idéia de grande influência foi a *representação por circuitos aritméticos*, inspirada em circuitos elétricos. Ela armazena f usando $x_1, ..., x_n$ e as constantes em f como entradas e indicando as operações por chaves (portas) de adição e multiplicação. O polinômio f que utilizamos de exemplo anteriormente seria representado como



O sucesso desse método ficou provado em 1989 quando E. Kaltofen [Kaltofen, 1989] demonstrou a fatoração em tempo polinomial sobre a representação em circuitos aritméticos, utilizando para tanto uma versão efetiva do teorema de irredutibilidade de Hilbert, assunto comentado no início do capítulo.

O segundo comentário que nos propusemos a fazer consiste em uma técnica bastante em voga não somente no que diz respeito à Álgebra Computacional, a *representação por caixa preta*. No nosso caso, um polinômio $f \in F[x_1, ..., x_n]$ é dado por uma subrotina dita "caixa preta" que, para uma entrada $a_1, ..., a_n \in F$ devolve o valor $f(a_1, ..., a_n) \in F$. De fato, partiremos de um polinômio em uma representação comum e construiremos sua "caixa preta", que poderá ser manipulada eficientemente, o que constitui exatamente o ponto crucial do método. Finalmente, a "caixa preta" de saída deve ser reconvertida em uma estrutura de formato legível via algoritmos de interpolação, veja [Díaz e Kaltofen, 1998] para mais informações.

APÊNDICE B DERIVAÇÕES

No capítulo que trata do Algoritmo de Gao para fatoração de polinômios em duas variáveis, utilizamos em uma de nossas demonstrações o conceito de extensão do operador derivada a uma extensão algébrica do corpo de funções racionais na variável y. Isso se justifica com base na Teoria de Operadores Diferenciais Algébricos, uma ferramenta de grande importância em Álgebra. Apresentaremos aqui uma discussão que nos leva diretamente a nossa aplicação, que foi fortemente inspirada no livro de S. Lang [Lang, 1965]. Refere-se o livro de N. Jacobson para leitores que desejam um tratamento de maior generalidade [Jacobson, 1964].

Iniciemos nossa discussão com a definição formal do que vem a ser um operador derivação em anel A.

Definição B.1. *Uma derivação D em um anel A é uma aplicação linear $D : A \to A$ que satisfaz a regra do produto usual, isto é, $D(xy) = xD(y) + yD(x)$.*

Exemplos elementares de derivação são as aplicações D_i, no anel de polinômios $k[x_1, ..., x_n]$ sobre o corpo k, que associam à variável x_i do polinômio sua derivada parcial usual. A partir delas, obtemos facilmente derivações para o seu corpo quociente simplesmente definindo

$$D(\frac{u}{v}) = \frac{vDu - uDv}{v^2}.$$

Concentraremo-nos em derivações em um corpo K. Uma derivação em K é dita trivial se $Dx = 0$, $\forall x \in K$. Analogamente, se $Dx = 0$, $\forall x \in k$, para certo subcorpo k de K, ela será dita trivial sobre o subcorpo k. Um derivação é sempre trivial sobre o subcorpo primo de K, pois $D(1) = D(1 \cdot 1) = 1 \cdot D(1) + 1 \cdot D(1) = 2D(1)$, logo $D(1) = 0$.

Consideremos o problema de estender derivações. Seja $L = K(\alpha_1, ..., \alpha_n)$ uma extensão finitamente gerada de K. Se $f \in K[x_1, ..., x_n]$, para indeterminadas

$x_1, ..., x_n$, denotaremos por $\frac{\partial f}{\partial \alpha_i}$ os polinômios $\frac{\partial f}{\partial x_i}$ avaliados no ponto $(\alpha_1, ..., \alpha_n)$. A pergunta que procuraremos responder a seguir é: dada uma derivação D em K, existirá uma derivação D^* em L coincidindo com D em K? É claro que, se $f \in K[x_1, ..., x_n]$ se anula quando aplicada em $(\alpha_1, ..., \alpha_n)$, então qualquer D^* nessas condições satisfaz

$$0 = D^* f(\alpha) = f^D(\alpha) + \sum (\frac{\partial f}{\partial \alpha_i}) D^* \alpha_i,$$

onde f^D denota o polinômio obtido da aplicação de D a todos os coeficientes de f e $\alpha = (\alpha_1, ..., \alpha_n)$. Note que, se a relação acima é satisfeita para o conjunto (finito) de geradores do ideal de $K[x_1, ..., x_n]$ formado pelos polinômios que se anulam em α, então, utilizando as regras de derivação, vê-se que ela será satisfeita por todos os polinômios nesse ideal, também denominado de ideal determinado por α. Mas essa condição necessária é também suficiente, conforme enuncia o teorema:

Teorema B.2. *Teorema de Extensão*

Seja D uma derivação sobre um corpo K. Sejam (α) um conjunto e $\{f_\nu(x)\}$ o conjunto de geradores do ideal determinado por α em $K[x]$. Então, se (u) é qualquer conjunto de elementos de $K(\alpha)$ satisfazendo as equações

$$0 = f_\nu^D(\alpha) + \sum \frac{\partial f_\nu}{\partial \alpha_i} u_i, \tag{B.1}$$

existe uma, e somente uma derivação D^* em $K(\alpha)$ tal que $D^* \alpha_i = u_i$ para todo i e que coincide com D em K.

Demonstração

A necessidade foi mostrada na discussão acima. Reciprocamente, se $g(\alpha)$, $h(\alpha)$ estão em $K(\alpha)$, e $h(\alpha) \neq 0$, verifica-se imediatamente que a aplicação D^* definida pelas fórmulas

$$D^* g(\alpha) = g^D(\alpha) + \sum \frac{\partial g}{\partial \alpha_i} u_i,$$

$$D^*(\frac{g(\alpha)}{h(\alpha)}) = \frac{h D^* g - g D^* h}{h^2}$$

está bem definida e é uma derivação em $K(\alpha)$, o que estabelece o resultado. □

Consideremos o caso especial em que (α) consiste de único elemento α, e seja D uma derivação em K.

Caso 1: α é algébrico e separável sobre K. Seja $f(x)$ o polinômio minimal de α, o polinômio irredutível sobre K que se anula em α. Pela separabilidade, $\frac{\partial f}{\partial x}(\alpha) \neq 0$. Obtemos também uma equação na forma (B.1) dada por

$$0 = f^D(\alpha) + u\ \frac{\partial f}{\partial x}(\alpha),$$

de tal modo que $u = -f^D(\alpha)/\frac{\partial f}{\partial x}(\alpha)$. Portanto, D é estendida a $K(\alpha)$ univocamente. Note que essa relação é exatamente a regra da cadeia, pois

$$\begin{aligned} 0 = D(f(\alpha)) = D(\sum_{i=1}^{n} a_i\alpha^i) &= \sum_{i=1}^{n} D(a_i\alpha^i) \\ &= \sum_{i=0}^{n} \frac{\partial a_i}{\partial x}\alpha^i + a_i i\alpha^{i-1}D\alpha \\ &= \sum_{i=0}^{n} \frac{\partial a_i}{\partial x}\alpha^i + D\alpha\ \sum_{i=1}^{n} i a_i\alpha^{i-1} = f^D(\alpha) + u\ \frac{\partial f}{\partial x}(\alpha), \end{aligned}$$

onde as propriedades (outras que a regra da cadeia) decorrem diretamente da definição de derivação. Em particular, se D é trivial em K, sua extensão será trivial em $K(\alpha)$.

Caso 2: α é transcendente sobre K. Então D é extensível e u pode ser escolhido arbitrariamente em $K(\alpha)$.

Caso 3: α é puramente inseparável sobre K, isto é, $\alpha^p - a = 0$ para certo $a \in K$. Então, D se estende a $K(\alpha)$ se, e somente se, $Da = 0$. Em particular, se D é trivial em K, então u pode ser escolhido arbitrariamente.

Vejamos como esse resultado é apropriado para a nossa proposição no capítulo 2: partimos dos operadores diferenciais usuais $\frac{\partial}{\partial x}$ e $\frac{\partial}{\partial y}$ em $F[x, y]$, onde F é um corpo (de fato, podemos considerá-los imediatamente como elementos em $\bar{F}[x, y]$). A partir do que chamamos de regra do quociente, chegamos a operadores diferenciais sobre o corpo $\bar{F}(y)$. Em particular, $\frac{\partial}{\partial y}$ coincide com a derivada de funções racionais que costumamos utilizar no Cálculo, enquanto que $\frac{\partial}{\partial x}$ é a derivação trivial.

Agora, consideremos L, o corpo de decomposição de um polinômio $f \in \bar{F}(y)[x]$ sobre $\bar{F}(y)$. Certamente, esse corpo é uma extensão finita, isto é, uma extensão algébrica e finitamente gerada de $\bar{F}(y)$. Logo, os operadores $\frac{\partial}{\partial y}$ e $\frac{\partial}{\partial x}$ podem ser estendidos a L aplicando um número finito de vezes o caso particular 1 descrito acima. A derivação D_y satisfaz equações como as do teorema de extensão e a derivação D_x é trivial em L.