R domínio de fatoração única implica R[x] também

Pedro Manfrim Magalhães de Paula

4 de Dezembro de 2013

Definição 1. Um domínio integral R com unidade é um *domínio de fatoração única* se

1. Todo elemento não nulo em R é uma unidade ou pode ser escrito como um produto finito de elementos irredutíveis de R.

2. A decomposição da parte (1) é única a menos de ordem e associados dos elementos irredutíveis.

A partir deste ponto assumiremos que todos os anéis R são domínios de fatoração única.

Já sabemos que anéis euclidianos são domínios de fatoração única. O oposto não ocorre pois, como veremos mais adiante, o anel $F[x_1, x_2]$ para um corpo F é um domínio de fatoração única que não é anel euclidiano (pois não é um domínio de ideais principais).

Em anéis comutativos podemos falar de maiores divisores comum, mas nem sempre podemos afirmar que estes existem. Em domínios de fatoração única podemos garantir esta existência pelo lema a seguir.

Lema 1. *Se $a, b \in R$, então a e b possuem um maior divisor comum $(a, b) \in R$. Ainda mais, se a e b são coprimos ($(a, b) = 1$), então sempre que $a|bc$ temos $a|c$.*

Demonstração. Suponha que $a = r_1...r_k...r_n$ e $b = s_1...s_k...s_m$ é uma decomposição de a e b tal que r_i, s_i são associados para $i \leq k$, e r_i, s_j não são associados $\forall i, j > k$, onde $k \geq 0$ (sempre podemos arranjar as fatorações de a e b para serem desta forma).

Defina $d = r_1...r_k$ (para $k = 0$ tomamos $d = 1$), então d divide a e b. Seja c divisor comum de a e b. Se $c \nmid d$, temos que a fatoração de c possui um irredutível f que não divide d. Então f divide algum r_i e algum s_j

para $i, j > k$, assim f é uma unidade ou r_i e s_j são associados que é uma contradição. Portanto $c|d$ e assim d é maior divisor comum de a e b.

Suponha que $(a, b) = 1$ e $a|bc$. Se a é unidade temos $a|c$. Se $a = r_1...r_k$ não é unidade, então existe $f = s_1...s_l \in R$ tal que $(p_1...p_n)(q_1...q_m) = bc = fa = (s_1...s_l)(r_1...r_k)$, onde os p_i, q_i, r_i, s_i são todos irredutíveis. Pela unicidade das fatorações e como nenhum r_i divide nenhum p_j, temos que para cada r_i existe um q_j associado. Logo $a|c$. $\square$

Corolário 1. *Se $a \in R$ é um elemento irredutível e $a|bc$, então $a|b$ ou $a|c$ (todo irredutível é primo).*

Demonstração. Se $b = r_1...r_n$ e $c = s_1...s_m$ é a decomposição de b e c em irredutíveis, então $a|bc \Rightarrow bc = da$ para algum $d = t_1...t_k \in R$. Logo $r_1...r_n s_1...s_m = t_1...t_k a$, e pela unicidade da decomposição temos que $a = r_i$ para algum i ou $a = s_j$ para algum j. Portanto $a|b$ ou $a|c$. $\square$

Queremos agora mostrar um análogo do Lema de Gauss para o anel $R[x]$ quando R é um domínio de fatoração única. Para isso precisamos definir o que seria um polinômio primitivo.

Definição 2. Dado $f(x) = a_0 + a_1x + ... + a_mx^m$ em $R[x]$ definimos o *conteúdo* de $f(x)$ como o conjunto dos maiores divisores comum de $a_0, ..., a_m$. Denotamos este conjunto por $c(f)$.

Como todo domínio de fatoração única é um domínio integral, temos que todos os maiores divisores comuns são associados. Logo o conteúdo de um polinômio $f(x) = a_0 + a_1x + ... + a_mx^m$ é formado pelos associados de um maior divisor comum de $a_0, ..., a_m$.

Definição 3. Um polinômio em $R[x]$ é dito *primitivo* se seu conteúdo é o conjunto das unidades.

Se $f(x) \in R[x]$, é fácil ver que podemos escrever $f(x) = af_1(x)$, onde $a \in c(f)$ e $f_1(x)$ é primitivo, e que esta decomposição é única a menos de associados de a e $f_1(x)$.

Lema 2. *O produto de polinômios primitivos em $R[x]$ é ainda um polinômio primitivo em $R[x]$.*

Demonstração. Sejam $p(x) = a_0 + ... + a_nx^n$ e $q(x) = b_0 + ... + b_mx^m$ e suponha que o lema seja falso. Então todos os coeficientes de $p(x)q(x)$ seriam divisíveis por um elemento de R que não é uma unidade, e assim seriam divisíveis por um irredutível d de R. Como $p(x)$ é primitivo, d não divide algum a_i. Seja a_j o primeiro coeficiente de $p(x)$ que não é divisível por d, e analogamente seja b_k o primeiro coeficiente de $q(x)$ que não é divisível por d. Para $p(x)q(x)$ o coeficiente de x^{j+k} é

$$c_{j+k} = a_j b_k + (a_{j+1}b_{k-1} + ... + a_{j+k}b_0) + (a_{j-1}b_{k+1} + ... + a_0 b_{j+k})$$

Pela escolha de a_j e b_k, $d|a_i$ para $i < j$ e $d|b_i$ para $i < k$, então $d|(a_{j-1}b_{k+1} + ... + a_0 b_{j+k})$ e $d|(a_{j+1}b_{k-1} + ... + a_{j+k}b_0)$. Pela suposição $d|c_{j+k}$, logo $d|a_j b_k$ contradição pois $d \nmid a_j$ e $d \nmid b_k$. Portanto temos o resultado. □

Corolário 2. *Se $f(x), g(x) \in R[x]$, então $c(fg) = c(f)c(g)$, onde $c(f)c(g) = \{ab/a \in c(f), b \in c(g)\}$.*

Demonstração. Podemos escrever $f(x) = af_1(x)$ e $g(x) = bg_1(x)$, onde $a \in c(f)$, $b \in c(g)$ e $f_1(x)$,$g_1(x)$ são primitivos. Então $f(x)g(x) = abf_1(x)g_1(x)$, e pelo Lema 2, $f_1(x)g_1(x)$ é primitivo. Logo o conteúdo de $f(x)g(x)$ contém ab, e como $c(f)c(g)$ contém todos os associados de seus elementos, temos $c(fg) = c(f)c(g)$. □

Por indução temos que o corolário se estende para um produto finito de polinômios, assim $c(f_1...f_n) = c(f_1)...c(f_n)$.

Como R é um domínio de fatoração única (em particular um domínio integral), R possui corpo de frações F. Assim podemos considerar $R[X]$ como um subanel de $F[x]$. Se $f(x) \in F[x]$, então $f(x) = a^{-1}f_0(x)$, onde $f_0(x) \in R[X]$ e $a \in R$.

Lema 3. *Se $f(x) \in R[x]$ é primitivo, então $f(x)$ é irredutível como elemento de $R[x]$ se e somente se $f(x)$ é irredutível como elemento de $F[x]$.*

Demonstração. ($\Rightarrow$) Suponha que $f(x)$ é irredutível em $R[x]$ mas é redutível em $F[x]$. Então $f(x) = g(x)h(x)$, onde $g(x), h(x) \in F[x]$ e possuem grau positivo. Sabemos que $g(x) = a^{-1}g_0(x)$, $h(x) = b^{-1}h_0(x)$, onde $a, b \in R$ e $g_0(x), h_0(x) \in R[x]$. Temos também que $g_0(x) = \alpha g_1(x)$, $h_0(x) = \beta h_1(x)$, onde $\alpha \in c(g_0)$, $\beta \in c(h_0)$ e $g_1(x)$, $h_1(x)$ são primitivos em $R[x]$. Logo $f(x) = (\frac{\alpha\beta}{ab})g_1(x)h_1(x)$, ou seja, $abf(x) = \alpha\beta g_1(x)h_1(x)$. Pelo Lema 2, $g_1(x)h_1(x)$ é primitivo, assim $ab \in c(abf) = c(\alpha\beta g_1 h_1) \ni \alpha\beta$. Portanto existe $u \in R$ unidade tal que $f(x) = ug_1(x)h_1(x)$, mas essa fatoração não é trivial já que o $grau(g_1) = grau(g) > 0$, $grau(h_1) = grau(h) > 0$ e as unidades de $F[x]$ não possuem grau positivo (contradição).

($\Leftarrow$) Suponha que $f(x)$ é irredutível em $F[x]$ e $f(x) = p(x)q(x)$ em $R[x]$. Então $f(x) = p(x)q(x)$ em $F[x]$, já que $R[x]$ é subanel de $F[x]$. Logo $p(x)$ ou $q(x)$ é unidade em $F[x]$. Como F é domínio integral, as unidades de $F[x]$ são as unidades de F, assim $p(x) \in F$ ou $q(x) \in F$. Mas $p(x), q(x) \in R[x]$, então $p(x)$ ou $q(x)$ é unidade de R. Logo $f(x)$ é irredutível em $R[x]$. □

Lema 4. *Se $p(x)$ é um polinômio primitivo em $R[x]$, então ele pode ser fatorado de maneira única como um produto de elementos irredutíveis em $R[x]$.*

Demonstração. Considerando $p(x)$ como elemento de $F[x]$, podemos fatorá-lo como $p(x) = p_1(x)...p_n(x)$, onde $p_1(x)$,...,$p_n(x)$ são polinômios irredutíveis em $F[x]$. Como $p_i(x) = a_i^{-1} f_i(x)$, onde $f_i(x) \in R[x]$ e $a_i \in R$; e mais, $f_i(x) = c_i q_i(x)$, onde $c_i \in c(f_i)$ e $q_i(x)$ é primitivo em $R[x]$. Temos que para cada i, $p_i(x) = \frac{c_i}{a_i} q_i(x)$, onde $a_i, c_i \in R$ e $q_i(x)$ é primitivo. Como $p_i(x)$ é irredutível em $F[x]$, $q_i(x)$ deve ser irredutível em $F[x]$, logo pelo Lema 3, $q_i(x)$ é irredutível em $R[x]$. Então

$$p(x) = p_1(x)...p_n(x) = \tfrac{c_1...c_n}{a_1...a_n} q_1(x)...q_n(x)$$

assim $a_1...a_n p(x) = c_1...c_n q_1(x)...q_n(x)$. Usando primitividade de $p(x)$ e de $q_1(x)...q_n(x)$, temos que o conteúdo da parte esquerda possui $a_1...a_n$ e da direita possui $c_1...c_n$. Logo $a_1...a_n$ e $c_1...c_n$ são associados, e assim existe unidade $u \in R$ tal que $p(x) = uq_1(x)...q_n(x)$. Temos então uma fatoração de $p(x)$ em $R[x]$ como um produto de irredutíveis.

A fatoração é única pois se $p(x) = r_1(x)...r_m(x)$, onde cada $r_i(x)$ é irredutível em $R[x]$, temos por primitividade de $p(x)$ que cada $r_i(x)$ é primitivo, e assim irredutível em $F[x]$ pelo Lema 3. Mas $F[x]$ é um domínio de fatoração única, logo os $r_i(x)$ são iguais aos $q_i(x)$ (a menos de associados) em alguma ordem. Portanto $p(x)$ tem uma fatoração única como produto de irredutíveis em $R[x]$. □

Teorema. *$R[x]$ é domínio de fatoração única.*

Demonstração. Seja $p(x) \in R[x]$, podemos escrever $p(x) = cp_1(x)$, onde $c \in c(p) \subset R$ e $p_1(x) \in R[x]$ é primitivo. Pelo Lema 4 podemos decompor $p_1(x)$ em um produto de irredutíveis em $R[x]$ de maneira única. Se $c = a_1(x)...a_n(x)$ em $R[x]$, temos que $0 = grau(c) = grau(a_1(x)) + ... + grau(a_n(x))$. Logo cada $a_i(x)$ tem grau 0, ou seja, é elemento de R. Assim as únicas fatorações de c em $R[x]$ são as formadas por elementos de R. Como R é domínio de fatoração única, existe uma única fatoração de c como produto de irredutíveis em R, e consequentemente em $R[x]$.

Pela unicidade da fatoração de $p(x)$ em $cp_1(x)$ e pela unicidade das fatorações de $p_1(x)$ e c, temos o resultado. □

Corolário 3. *$R[x_1, ..., x_n]$ é domínio de fatoração única.*

Demonstração. Usando o fato de R ser domínio de fatoração única temos que $R[x_1]$ também é, como $R[x_1, x_2] = R[x_1][x_2]$ usamos indução e temos o resultado. □

Corolário 4. *Se F é corpo, então $F[x_1, ..., x_n]$ é domínio de fatoração única.*

Bibliografia

[1] I. N. Herstein *Topics in Algebra*, JOHN WILEY & SONS, pp. 163 - 166