Fatorar $\mathbb{Q}[x]$ reduzindo em fatores de $\mathbb{Z}[x]$;

Se $f(x) \in \mathbb{Q}[x]$, então $cf(x)$ tem coeficientes inteiros para algum inteiro $c \neq 0$.

Exemplo: $f(x) = x^5 + \frac{2}{3}x^4 + \frac{3}{4}x^3 - \frac{1}{6}$

Assim o denominador comum de $f(x)$ é 12, e $12 \cdot f(x)$ tem coeficientes inteiros:

$$12 f(x) = 12 \cdot \left[x^5 + \frac{2}{3}x^4 + \frac{3}{4}x^3 - \frac{1}{6}\right]$$

$$= 12x^5 + 8x^4 + 9x^3 - 2$$

Teorema 4.21: Teste de raízes racionais

Temos $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ sendo um polinômio com coeficientes inteiros. Se $r \neq 0$ e r/s é um número racional (em termos menores) é uma raiz de $f(x)$, então $r | a_0$ e $s | a_n$.

Exemplo 1: As possíveis raízes em $\mathbb{Q}$ de $f(x)$,

$f(x) = 2x^4 + x^3 - 21x^2 - 14x + 12$, são da mesma forma que r/s onde r é um dos $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6$, ou ± 12 (os divisores constantes de 12) e s é $\pm 1, \pm 2$ (os divisores do coeficiente de maior grau, 2).

$f(x) = 2x^4 + x^3 - 21x^2 - 14x + 12$

$\hookrightarrow \pm 1, \pm 2$ $\qquad$ $\hookrightarrow \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$

Então as raízes racionais no teste de redução na pesquisa por raízes de $f(x)$ para esta lista finita de possibilidades:

Forma: $\frac{r}{s} = \frac{(1,-1,2,-2,3,-3,4,-4,6,-6,12,-12) \in \mathbb{Z}}{(1,-1,2,-2) \in \mathbb{Z}}$

• $\frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{3}{2} \in \mathbb{Q}$.

É entediante, mas simplesmente substituir cada um desses em $f(x)$ para encontrar que $(-3, \frac{1}{2})$ são as únicas raízes de $f(x)$ em $\mathbb{Q}$.

Pelo Teorema fator, ambos:

$x-(-3) = x+3$ e $x-\frac{1}{2}$ são fatores de $f(x)$.

Então:

$$f(x) = (x+3).\left(x-\frac{1}{2}\right).(2x^2-4x-8)$$

A fórmula quadrática mostra que as raízes de $2x^2-4x-8$ são $(1 \pm \sqrt{5})$, que não pertence a $\mathbb{Q}$. Então, $2x^2-4x-8$ é irredutível em $\mathbb{Q}[x]$ pelo corolário 4.19. Então, temos fatorado $f(x)$ como um produto de polinômios irredutíveis em $\mathbb{Q}[x]$.

Exemplo 2: As únicas raízes possíveis de $g(x) = x^3+4x^2+x-1$ em $\mathbb{Q}$ são $(1$ e $-1)$. Por quê?

$\begin{matrix} \hookrightarrow \pm 1 & & & & \hookrightarrow \pm 1 \end{matrix}$

$\pm 1, \pm 1, \frac{+1}{1}, \frac{-1}{1} = +1$ e -1, temos que:

$g(1) = 1 + 4 + \cancel{1} - \cancel{1} = 5$
$g(-1) = -1 + 4 - 1 - 1 = 1$

Então $g(x)$ é irredutível em $\mathbb{Q}[x]$ pelo corolário 4.19.

<u>Corolário 4.19</u>: Temos F sendo um corpo e temos $f(x) \in F[x]$ sendo um polinômio de grau 2 ou 3. Então $f(x)$ é irredutível em $F[x]$ se e somente se $f(x)$ não tem raízes em F.

Se $f(x) \in \mathbb{Q}[x]$, então $cf(x)$ tem coeficientes inteiros para algum inteiro $c \neq 0$. Qualquer fatoração de $cf(x)$ em $\mathbb{Z}[x]$ conduzida pela fatoração de $f(x)$ em $\mathbb{Q}[x]$, então ela aparece que o teste para irredutibilidade em $\mathbb{Q}[x]$ pode ser restrito para polinômios com coeficientes inteiros. Contudo, temos a primeira regra da possibilidade que um polinômio com coeficientes inteiros poderia ser fator em $\mathbb{Q}[x]$, mas não em $\mathbb{Z}[x]$.

Nesta ordem, temos o lema.

<u>Lema 4.22</u>: Temos $f(x), g(x), h(x) \in \mathbb{Z}[x]$ com $f(x) = g(x)h(x)$. Se p é um primo que divide cada coeficiente de $f(x)$, então p divide cada coeficiente de $g(x)$ ou p divide cada coeficiente de $h(x)$.

Teorema 4.23: Temos $f(x)$ sendo um polinômio com coeficientes inteiros. Então $f(x)$ como um fator de produtos de polinômios de grau m e n em $\mathbb{Q}[x]$, se e somente se, $f(x)$ fatores como um produto de polinômios de graus m e n em $\mathbb{Z}[x]$.

Exemplo 3: Afirmamos que $f(x) = x^4 - 5x^2 + 1$ é irredutível em $\mathbb{Q}[x]$. A prova é por contradição.

Se $f(x)$ é irredutível, ele pode ser fatorado como o produto de 2 polinômios não constantes em $\mathbb{Q}[x]$. Se algum desses fatores tiver grau 1, então $f(x)$ tem uma raiz em $\mathbb{Q}$.

Mas o teste da raiz racional mostra que $f(x)$ não tem raiz em $\mathbb{Q}$. (As únicas possibilidades são ± 1, e nenhuma é raiz).

Assim se $f(x)$ é redutível, a única possibilidade de fatoração é um produto de duas quadráticas, neste caso o Teorema 4.23 mostra que existe uma fatoração em $\mathbb{Z}[x]$.

Além disso, existe uma fatoração como um produto de mônicos quadráticos em $\mathbb{Z}[x]$, e

$$(x^2+ax+b)(x^2+cx+d) = x^4-5x^2+1$$

com $a, b, c, d \in \mathbb{Z}$.

Multiplicando o lado esquerdo, temos:

$$x^4 + (a+c)x^3 + (ac+b+d)x^2 + (bc+da)x + bd =$$
$$x^4 + 0x^3 - 5x^2 + 0x + 1$$

Como os polinômios iguais, tem coeficientes iguais, então:

$a + c = 0 \longrightarrow a = -c$, então

$ac + b + d = -5$

$bc + ad = 0 \longrightarrow bc = -da$

$bd = 1$

$bc = -d(-c)$

$b\cancel{c} = d\cancel{c}$

$b = d$

$bd = 1$

$b.b = 1$

$b = 1$

$b = -1$

$ac + b + d = -5$

$-c.c + b + b = -5$

$-c^2 + 2b = -5 \longrightarrow -c^2 + 2.1 = -5$

$-c^2 = -5 - 2$

$-c^2 = -7 \ (-1)$

$c^2 = 7$

$c = \sqrt{7}$

Se $b = -1$

$c = \sqrt{3}$

Não existe inteiros $\sqrt{3}$ ou $\sqrt{7}$, e então uma fatoração de $f(x)$ como produto de quadráticas em $\mathbb{Z}[x]$, e, então em $\mathbb{Q}[x]$ é impossível. Portanto, $f(x)$ é irredutível em $\mathbb{Q}[x]$.

<u>Teorema 4.24</u>: Critério de Eisenstein

Temos $f(x) = a_n x^n + \dots + a_1 x + a_0$ sendo um polinômio não constante com coeficientes inteiros. Se existe um primo "p" sendo que "p" divide cada $a_0, a_1, \dots, a_{n-1}$. Mas "p" não divide a_n e "p^2" não divide a_0, então $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Exemplo 4: O polinômio $x^{17}+6x^{13}-15x^4+3x^2-9x+12$ é irredutível em $\mathbb{Q}[x]$ pelo critério de Eisenstein com $p=3$.

i) polinômio não constante com coeficientes inteiros,

ii) "p": $p \mid 12$, $p \mid 9$, $p \mid 3$, $p \mid 15$, $p \mid 6$, se $p=3$,

$p \nmid 1 \rightarrow 3 \nmid 1$.

$p^2 \nmid 12 \rightarrow 3^2 \nmid 12$.

Então $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Exemplo 5: O polinômio x^9+5 é irredutível em $\mathbb{Q}[x]$ pelo critério de Eisenstein, com $p=5$.

$p \mid 5$, $p \nmid 1$ e $p^2 \nmid 5$

Similarmente, x^n+5 é irredutível em $\mathbb{Q}[x]$ para cada $n \geq 1$. Assim:

"Existem polinômios irredutíveis de cada grau em $\mathbb{Q}[x]$."

Embora o critério de Eisenstein é muito eficiente, muitos polinômios não pode ser aplicados. Nestes casos é necessário outras técnicas, um método envolvido é a redução polinomial em "mod p".

Temos "p" sendo um primo positivo, para cada inteiro a, temos $[a]$ que denota a consequência classe de a em $\mathbb{Z}_p$. Se $f(x) = a_k x^k + \dots + a_1 x + a_0$ é um polinômio com coeficientes inteiros, temos $\bar{f}(x)$ denota o polinômio:

$$[a_k]x^k + \dots + [a_1]x + [a_0] \text{ em } \mathbb{Z}_p[x]$$

Por exemplo, se $f(x) = 2x^4 - 3x^2 + 5x + 7$ em $\mathbb{Z}[x]$, então em $\mathbb{Z}_3[x]$,

mod3 mod3 mod3

$$\bar{f}(x) = [2]x^4 - [3]x^2 + [5]x + [7]$$

$$= [2]x^4 - [0]x^2 + [2]x + [1]$$
$$= [2]x^4 + [2]x + [1]$$

Observamos que $f(x)$ e $\bar{f}(x)$ tem os mesmo grau, isto sempre acontecerá para casos quando temos coeficientes de $f(x)$ não é divisível por "p" (então temos que os coeficientes de $\bar{f}(x)$ não irá ser zero na classe $\mathbb{Z}_p$).

<u>Teorema 4.25</u>: Temos $f(x) = a_k x^k + \dots + a_1 x + a_0$ sendo um polinômio com coeficientes inteiros, e temos "p" sendo um primo positivo que não divide a_k. Se $\bar{f}(x)$ é irredutível em $\mathbb{Z}_p[x]$, então $f(x)$ é irredutível em $\mathbb{Q}[x]$.

A utilidade do teorema 4.25 depende sobre o fato: para cada inteiro k não negativo, existem finitamente muitos polinômios de grau k em $\mathbb{Z}_p[x]$.

Portanto, isto sempre é possível, em teoria, determinar se um dado polinômio em $\mathbb{Z}p[x]$ é irredutível pela verificação dos números finitos de fatores possíveis. Dependendo do tamanho de "p" e do grau de $f(x)$, isto pode ser feito em uma quantidade razoável de tempo.

Exemplo 6: Mostrar que $f(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$ é irredutível em $\mathbb{Q}[x]$, podemos reduzir em mod 2.

Em $\mathbb{Z}_2[x]$, $\bar{f}(x) = x^5 + x^2 + 1$. Isto é fácil ver que $\bar{f}(x)$ não tem raízes em $\mathbb{Z}_2$ e então não tem primeiro grau de fatores em $\mathbb{Z}_2[x]$.

Temos que ± 1 não é raiz de $\bar{f}(x)$, e $\bar{f}(x) = [1]x^5 + 1[x^2] + [1]$.

Somente polinômios quadráticos em $\mathbb{Z}_2[x]$ são: x^2, x^2+x, x^2+1, e x^2+x+1.
Contudo, se x^2, $x^2+x = x(x+1)$, ou $x^2+1 = (x+1)(x+1)$ é um fator, então $\bar{f}(x)$ poderia ter um primeiro-grau de fator, mas isto não acontece.

Pode-se usar divisão para mostrar que o quadrado restante de, x^2+x+1 não é um fator de $\bar{f}(x)$.

Finalmente, $\bar{f}(x)$ não pode ter um fator de grau 3 ou 4 (se ele tivesse, os outros

poderia ter grau 2 e 1, que é impossível.
Portanto, $f(x)$ é irredutível em $\mathbb{Z}_2[x]$, então, $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Atenção: Se um polinômio em $\mathbb{Z}[x]$ é reduzido "mod p" para um polinômio que é redutível em $\mathbb{Z}_p[x]$. então nenhuma conclusão podemos ter do teorema 4.25.
Infelizmente, existem muitos "p" para qual a redução de $f(x)$ é redutível em $\mathbb{Z}_p[x]$, sempre quando $f(x)$ é atualmente irredutível em $\mathbb{Q}[x]$.
Consequentemente, isto pode acontecer mais vezes para aplicar o teorema 4.25 mais do que parece.