

Tarea final AC

Algoritmo de la división

Código

```
DIVISIÓN( $f_1, \dots, f_s, f$ ):  
1   $q_1 := 0; \dots; q_s := 0; r := 0 \ p := f$   
2  while  $p \neq 0$  do  
3       $i := 1$   
4      divisionoccurred=false  
5      while  $i \leq s$  and divisionoccurred=false do  
6          if  $\text{lt}(f_i)$  divides  $\text{lt}(p)$  then  
7               $q_i := q_i + \text{lt}(p) / \text{lt}(f_i)$   
8               $p := p - (\text{lt}(p) / \text{op}(f_i)) f_i$   
9              divisionoccurred=true  
10         else  
11              $i := i + 1$   
12         if divisionoccurred = false then  
13              $r := r + \text{lt}(p) \ p := p - \text{lt}(p)$   
14 return  $q_1, \dots, q_s, r$ 
```

Ejemplo del libro

Sean $f_1 = xy - 1$, $f_2 = y^2 - 1$, con orden lexicográfico. Si dividimos $f = xy^2 - x$ por $F = (f_1, f_2)$ obtenemos:

$$xy^2 - x = y(xy - 1) + 0(y^2 - 1) + (-x + y)$$

Si tomamos $F = (f_2, f_1)$, obtenemos:

$$xy^2 - x = x(y^2 - 1) + 0(xy - 1) + 0$$

En python:

```
R.<x,y> = PolynomialRing(RR, 2, "xy", order = "lex")
f = x*y^2-x; f1=x*y-1; f2=y^2-1

[q1,q2], r = div_poly([f1,f2],f)
print("Caso 1:")
show(html(f"${f} = {q1} ({f1}) + {q2} ({f2}) + ({r})$"))
print("Caso 2:")
f = x*y^2-x
f1=x*y-1
f2=y^2-1

[q2,q1], r = div_poly([f2,f1],f)
show(html(f"${f} = {q2} ({f2}) + {q1} ({f1}) + {r}$"))
```

Ejemplo del libro

Caso 1:

$$x * y^2 - x = x(y^2 - 1.0000000000000000) + 0(x * y - 1.0000000000000000) + 0$$

Caso 2:

$$x * y^2 - x = y(x * y - 1.0000000000000000) + 0(y^2 - 1.0000000000000000) + (-x + y)$$

Aplicado a polinomios aleatorios

```
R.<x_1,x_2,x_3,x_4> = PolynomialRing(GF(7), order="lex")
```

```
f = R.random_element(degree=4, terms = 4)
```

```
F = [R.random_element(degree=1, terms=2) for _ in range(3)]
```

```
Q, r = div_poly(F, f, R = R)
```

```
show(html(f"""
$$
\\begin{{align*}}
f = &{f} \\ \\ \\
\\sum_i q_i f_i + r = &{
    sum([q*f for q,f in zip(Q,F)]) + r
} \\ \\ \\
f_1 = &{F[0]} \\ \\text{quad} \\ \\text{quad} q_1 = {Q[0]} \\ \\ \\
f_2 = &{F[1]} \\ \\text{quad} \\ \\text{quad} q_2 = {Q[1]} \\ \\ \\
f_3 = &{F[2]} \\ \\text{quad} \\ \\text{quad} q_3 = {Q[2]} \\ \\ \\
r = &{r}
\\end{{align*}}
$$
"""))
```

Aplicado a polinomios aleatorios

$$f = 3 * x_1 * x_2 + x_3^2 + 3 * x_3$$

$$\sum_i q_i f_i + r = 3 * x_1 * x_2 + x_3^2 + 3 * x_3$$

$$f_1 = -x_2 + 3 * x_4$$

$$q_1 = -3 * x_1$$

$$f_2 = -2 * x_3 - 3$$

$$q_2 = 3 * x_3 + 1$$

$$f_3 = -x_2 - 1$$

$$q_3 = 0$$

$$r = 2 * x_1 * x_4 + 3$$