

Factoring in $\mathbb{Q}(\alpha)[x]$ using Trager's algorithm.

Copyright Michael Monagan, Fall 2023.

```
> m := z^2+z+1;
                                m := z^2 + z + 1
> alias( alpha=RootOf(m,z) );
                                alpha
> N := proc(f) resultant(m,subs(alpha=z,f),z) end;
                                N := proc(f) resultant(m, subs(alpha = z, f), z) end proc
> f := x^3-x^2+x-alpha*x^2+x*alpha-alpha;
                                f := x^3 - x^2 + x - alpha x^2 + x alpha - alpha
> f := unapply(f,x);
                                f := x -> x^3 - x^2 + x - alpha x^2 + x alpha - alpha
> N(f(x));
                                (x^2 - x + 1)^2 (1 + x + x^2)
```

Obviously $N(f(x))$ is not square-free. Let's try with $s = 2$.

```
> r := N(f(x-2*alpha));
                                r := 24 x^4 + 53 x^3 + 112 x^2 + 93 x + 63 + 5 x^5 + x^6
> gcd(r,diff(r,x));
                                1
> factor(r);
                                (1 + x + x^2) (x^2 + x + 7) (x^2 + 3x + 9)
> b1,b2,b3 := op(%);
                                b1, b2, b3 := 1 + x + x^2, x^2 + x + 7, x^2 + 3x + 9
> f1 := gcd( f(x-2*alpha), b1, 'q' );
                                f1 := x - alpha
> q;
                                x^2 - x - 6x alpha - 9 - 6 alpha
> f2 := gcd( q, b2, 'f3' );
                                f2 := x - 1 - 3 alpha
> f3;
                                x - 3 alpha
> f1 := subs( x=x+2*alpha, f1 );
> f2 := subs( x=x+2*alpha, f2 );
> f3 := subs( x=x+2*alpha, f3 );
> f(x)=f1*f2*f3;
                                x^3 - x^2 + x - alpha x^2 + x alpha - alpha = (x + alpha) (x - alpha - 1) (x - alpha)
```

```
> evala( Expand(f1*f2*f3) );  
x3 - x2 + x - αx2 + xα - α  
=   
> factor(f(x),alpha);  
(x + α) (-x + α + 1) (-x + α)
```