Handouts

November 21, 2023 8:46 AM

Goal factor $f(x,\alpha)$ over $\mathbb{Q}(\alpha)$.

$\alpha/m(z)$	$f(x,\alpha)$	$N(f(x,\alpha))$
$\sqrt{2}$	$x^2+(1+2\sqrt{2})x+2+\sqrt{2}$ $=(x+\sqrt{2})(x+\sqrt{2}+1)$	$x^4+2x^3-3x^2-4x-2$ $=(x^2-2)(x^2+2x-1)$
$\sqrt{2}$	$x^2-2=(x-\sqrt{2})(x+\sqrt{2})$	$x^4-4x^2+4=(x^2-2)^2$
$\sqrt[4]{2}$	$x^2-(\sqrt{2}+\sqrt[4]{2})x+\sqrt[4]{2}^3)$ $=(x-\sqrt{2})(x-\sqrt[4]{2})$	$x^8-4x^6+2x^4+8x-8$ $=(x^2-2)^2(x^4-2)$
z^2+z+1	$x^3-zx^2-zx-z-1$ $=(x+z+1)(x-z)(x-z-1)$	$x^6+x^5+2x^4+x^3+2x^2+x+1$ $=(x^2+x+1)^2(x^2-x+1)$

$\gcd(f, x^2-2) = x+\sqrt{2}$ ✓ ✓

$\gcd(f, x^2+2x+1) = x+\sqrt{2}+1.$

factor N over $\mathbb{Q}$.

$\gcd(f = x^2-2, x^2-2) = x^2-2.$ ✗

$\gcd(f, x^2-2) = x-\sqrt{2}$ ✓ $\gcd(f, x^4-2) = x-\sqrt[4]{2}$ ✓

$\gcd(f, x^2+x+1) = x^2+x+1.$ ✗

$\gcd(f, x^2-x+1) = x-z-1.$ ✓

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

```
> 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;
```

$$N := \mathbf{proc}(f)\ \ resultant(m, subs(\alpha = z, f), z)\ \ \mathbf{end\ proc}$$

```
> 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);
```

$$f := x \rightarrow x^3 - x^2 + x - \alpha x^2 + x\alpha - \alpha$$

```
> 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));
```

$$r := 24x^4 + 53x^3 + 112x^2 + 93x + 63 + 5x^5 + x^6$$

```
> gcd(r,diff(r,x));
```

$$1$$

```
> factor(r);
```

$$(\underline{1 + x} + x^2)\ (x^2 + x + 7)\ (x^2 \underline{+ 3x} + 9)$$

```
> b1,b2,b3 := op(%);
```

$$b1, b2, b3 := 1 + x + x^2, x^2 + x + 7, x^2 + 3x + 9$$

↗ deg 3 in α

```
> f1 := gcd( f(x-2*alpha), b1, 'q' );
```

$$f1 := x - \alpha$$

gcd(f, b2)

gcd(f, b3)

↑ degree 3 in x.

```
> q;
```

$q = f/b_1$

$$x^2 - x - 6x\alpha - 9 - 6\alpha$$

```
> 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) );
```

$$x^3 - x^2 + x - \alpha x^2 + x \alpha - \alpha$$

```
> factor(f(x),alpha);
```

$$(x + \alpha)\ (-x + \alpha + 1)\ (-x + \alpha)$$

↑ factor f over $\mathbb{Q}(\alpha)$.