```
> f := (x-2/3)*(x^2+1)*(x^2+x+1);
```

$$f := \left(x - \frac{2}{3}\right) \left(x^2 + 1\right) \left(x^2 + x + 1\right) \qquad (1)$$

```
> roots(f);
```

$$\left[\left[\frac{2}{3}, 1\right]\right] \qquad (2)$$

```
> Roots(f) mod 5;
```

$$[[2, 1], [3, 1], [4, 1]] \qquad (3)$$

```
> 2/3 mod 5;
```

$$4 \qquad (4)$$

```
> Roots(f) mod 7;
```

$$[[2, 1], [3, 1], [4, 1]] \qquad (5)$$

```
> 2/3 mod 7;
```

$$3 \qquad (6)$$

```
> Roots(x^2+x+1) mod 7;
```

$$[[2, 1], [4, 1]] \qquad (7)$$

```
> Roots(f) mod 11;
```

$$[[8, 1]] \qquad (8)$$

```
> Roots(f) mod 13;
```

$$[[3, 1], [5, 2], [9, 1], [8, 1]] \qquad (9)$$

```
> 2/3 mod 13;
```

$$5 \qquad (10)$$

```
> f;
```

$$\left(x - \frac{2}{3}\right) \left(x^2 + 1\right) \left(x^2 + x + 1\right) \qquad (11)$$

```
> alias( i = RootOf(z^2+1) );
```

$$i \qquad (12)$$

```
> roots(f,i); # over Q(i)
```

$$\left[\left[\frac{2}{3}, 1\right], [-i, 1], [i, 1]\right] \qquad (13)$$

```
> alias(omega=RootOf(z^2+z+1));
```

$$i, \omega \qquad (14)$$

```
> roots(f,omega); # over Q(omega)
```

$$\left[[-1 - \omega, 1], \left[\frac{2}{3}, 1\right], [\omega, 1]\right] \qquad (15)$$

```
> factor(f,omega);
```

$$-\frac{(x + 1 + \omega)\ (3\,x - 2)\ \left(x^2 + 1\right)\ (-x + \omega)}{3} \qquad (16)$$

```
> roots(f,{i,omega}); # over Q(i,omega)
```

$$\left[[-1 - \omega, 1], [i, 1], \left[\frac{2}{3}, 1\right], [-i, 1], [\omega, 1]\right] \qquad (17)$$

```
> gamma = i + omega;
```

$$\gamma = i + \omega \qquad (18)$$

```
> m := evala(Minpoly(i+omega,z));
```

(19)

$$m := z^4 + 2z^3 + 5z^2 + 4z + 1 \tag{19}$$

```
> alias(gamma=RootOf(m,z));
```

$$i, \omega, \gamma \tag{20}$$

```
> roots(f,gamma); # over Q(gamma)
```

$$\left[\left[\frac{2}{3}, 1\right], \left[-2\gamma^3 - 3\gamma^2 - 9\gamma - 4, 1\right], \left[2\gamma^3 + 3\gamma^2 + 8\gamma + 3, 1\right], \left[-2\gamma^3 - 3\gamma^2 - 8\gamma - 4, 1\right], \left[2\gamma^3 + 3\gamma^2 + 9\gamma + 4, 1\right]\right] \tag{21}$$

```
> F := [ x^2+1, y^2+y+1, z-x-y ];
```

$$F := \left[x^2 + 1, y^2 + y + 1, z - x - y\right] \tag{22}$$

```
> map(Groebner[LeadingMonomial],F,plex(z,y,x));
```

$$\left[x^2, y^2, z\right] \tag{23}$$

So F is alread a Groebner basis in lex order with z>x,y.   We want to eliminate x,y to get the minimal polynomial

```
> G := Groebner[Basis]( F, plex(y,x,z) );
```

$$G := \left[z^4 + 2z^3 + 5z^2 + 4z + 1, -2z^3 - 3z^2 + x - 9z - 4, 2z^3 + 3z^2 + y + 8z + 4\right] \tag{24}$$

I intersect Q[z]

```
> G[1];
```

$$z^4 + 2z^3 + 5z^2 + 4z + 1 \tag{25}$$

```
> f;
```

$$x^2 + x + 1 \tag{26}$$

```
> Roots(f) mod 5;
```

$$[\,] \tag{27}$$

```
> Roots(f) mod 11;
```

$$[\,] \tag{28}$$

```
> Roots(f,i) mod 11;  # Z11[z]/z^2+1
```

$$[[3i + 5, 1], [8i + 5, 1]] \tag{29}$$

```
> Roots(f,omega) mod 11;
```

$$[[10\omega + 10, 1], [\omega, 1]] \tag{30}$$

```
> f;
```

$$x^2 + x + 1 \tag{31}$$

```
> f := x^2+x+1;
```

$$f := x^2 + x + 1 \tag{32}$$

```
> Factor(f) mod 2;
```

$$x^2 + x + 1 \tag{33}$$

```
> Eval(f,x=1) mod 2;
```

$$1 \tag{34}$$

```
> Eval(f,x=0) mod 2;
```

$$1 \tag{35}$$

```
> alias(omega=RootOf(f,x));
```

$$i, \omega, \gamma, \alpha \tag{36}$$

```
> # R = Z2[z]/(z^2+z+1) = {1,z,z+1,0} is a finite field with 4
```

elements

```
> R := [0,1,omega,omega+1];
```

$$R := [0, 1, \omega, \omega + 1] \quad \textbf{(37)}$$

```
> Y := [seq( Eval(f,x=R[k]) mod 2, k=1..4 )];
```

$$Y := [1, 1, 0, 0] \quad \textbf{(38)}$$

```
> f;
```

$$x^2 + x + 1 \quad \textbf{(39)}$$

```
> Interp( R, Y, x ) mod 2;
```

$$x^2 + x + 1 \quad \textbf{(40)}$$

```
> m := Randprime(10,z) mod 2;
```

$$m := z^{10} + z^6 + z^2 + z + 1 \quad \textbf{(41)}$$

```
> alias(alpha=RootOf(m,z));
```

$$i, \omega, \gamma, \alpha \quad \textbf{(42)}$$

```
> X := [seq( alpha^k, k=2..6 )];
```

$$X := [\alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6] \quad \textbf{(43)}$$

```
> Y := [seq( Eval(f,x=X[k]) mod 2, k=1..5 )];
```

$$Y := [\alpha^4 + \alpha^2 + 1, \alpha^6 + \alpha^3 + 1, \alpha^8 + \alpha^4 + 1, \alpha^6 + \alpha^5 + \alpha^2 + \alpha, \alpha^8 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1] \quad \textbf{(44)}$$

```
> Interp( X, Y, x ) mod 2;
```

$$x^2 + x + 1 \quad \textbf{(45)}$$