```
> restart:
  #f:=expand((x+sqrt(2+sqrt(2)))*(x+sqrt(2-sqrt(2)))*(x-sqrt(2+sqrt
  (2)))*(x-sqrt(2-sqrt(2))));
```

```
> f := factor(x^4-2);
```

$$f := x^4 - 2 \tag{1}$$

```
> alias(y1 = RootOf(f,x));
```

$$y1 \tag{2}$$

```
> facs_y1:=evala(Factor(f,y1));
```

$$facs_y1 := \left(x^2 + y1^2\right)\ (x + y1)\ (x - y1) \tag{3}$$

```
> f1 := op(1,facs_y1);
```

$$f1 := x^2 + y1^2 \tag{4}$$

```
> alias(y2 = RootOf(f1,x));
```

$$y1, y2 \tag{5}$$

```
> facs_y1_y2 := evala(Factor(f,{y2,y1}));
```

$$facs_y1_y2 := (x + y2)\ (x - y2)\ (x + y1)\ (x - y1) \tag{6}$$

```
> facs_z := subs({y1=z1,y2=z2},facs_y1_y2);
```

$$facs_z := (x + z2)\ (x - z2)\ (x + z1)\ (x - z1) \tag{7}$$

```
> f1_z := subs({y1=z1,x=z2},f1);f_z := subs(x=z1,f);
```

$$f1_z := z1^2 + z2^2$$

$$f_z := z1^4 - 2 \tag{8}$$

```
> F := expand(facs_z);
```

$$F := x^4 - x^2\,z1^2 - x^2\,z2^2 + z1^2\,z2^2 \tag{9}$$

```
> expand(rem(F,f1_z,z2));
```

$$x^4 - z1^4 \tag{10}$$

```
> rem(%,f_z,z1);
```

$$x^4 - 2 \tag{11}$$

```
> evala(Factor(f1,{y2,y1}));
```

$$(x + y2)\ (x - y2) \tag{12}$$

```
> for i from 1 to 4 do ry||i := -subs(x=0,op(i,facs_y1_y2)); od;
```

$$ry1 := -y2$$

$$ry2 := y2$$

$$ry3 := -y1$$

$$ry4 := y1 \tag{13}$$

```
> # check a root by substituting back
> for i from 1 to 4 do evala(subs(x=ry||i, f)); od;
```

$$0$$

$$0$$

$$0$$

$$0 \tag{14}$$

```
> # Now we wish to identify an automorphism which maps y1 -> y2
  # First, find the possible images of y2
> map_y1 := ry2;
```

$$map_y1 := y2 \tag{15}$$

```
> map_f1 := evala(subs(y1 = map_y1, f1));
```

$$map_f1 := x^2 - y1^2 \quad (16)$$

```
> # map_f1 is a factor of f over Q(y1,y2)
  evala(Factor(map_f1, {y2,y1})); # could have plugged in roots
```

$$(x + y1)\,(x - y1) \quad (17)$$

```
> # Possible images for y2 are y1, -y1
  map_y2 := ry3;
```

$$map_y2 := -y1 \quad (18)$$

```
> evala(subs(x=map_y2,map_f1));
```

$$0 \quad (19)$$

```
> # Compute the permutation of the roots by mapping them
  for i from 1 to 4 do
      map_ry||i := evala(subs({y1=map_y1,y2=map_y2},ry||i));
      # print(i);
      print(sort(map_ry||i));
      # print("Check if root of f",
              #evala(subs(x=map_ry||i,f)));
      for j from 1 to 4 do
          if eval(map_ry||i - ry||j) = 0 then print(cat(i,"->",j));
  fi;
      od;
  end do:
```

$$\begin{array}{c} y1 \\ 1->4 \\ -y1 \\ 2->3 \\ -y2 \\ 3->1 \\ y2 \\ 4->2 \end{array} \quad (20)$$

```
> # Compute the norm of a random element
> u:=  z1+2*z2; #RandomTools['Generate'](polynom(integer(range=-1.
  .1),{z1,z2}));
```

$$u := z1 + 2\,z2 \quad (21)$$

```
> norm_u_y2:=evala(expand(subs({z1=y1,z2=y2},u) * subs({z1=y1,z2=-
  y2},u)));
```

$$norm_u_y2 := 5\,y1^2 \quad (22)$$

```
> norm_u_y2_y1:=1: for i from 1 to 4 do
                       norm_u_y2_y1 := evala(expand(norm_u_y2_y1 *
  subs(y1=ry||i, norm_u_y2)));
                    od:
> norm_u_y2_y1;
```

$$2500 \quad (23)$$

```
> ifactor(%);
```

$$(2)^2\,(5)^4 \tag{24}$$

```
> norm_ux_y2:=evala(expand((x - subs({z1=y1,z2=y2},u)) * (x - subs(
  {z1=y1,z2=-y2},u))));
```

$$norm_ux_y2 := x^2 - 2\,x\,y1 + 5\,y1^2 \tag{25}$$

```
> evala(Factor(norm_ux_y2,{y2,y1}));
```

$$(x - y1 + 2\,y2)\,(x - 2\,y2 - y1) \tag{26}$$

```
> norm_ux_y2_y1:=1: for i from 1 to 4 do
                    norm_ux_y2_y1 := evala(expand(norm_ux_y2_y1
                                                  * subs(y1=
  ry||i, norm_ux_y2)));
                  od:
> f_min:=norm_ux_y2_y1;
```

$$f_min := x^8 + 28\,x^4 + 2500 \tag{27}$$

```
> factor(%);
```

$$x^8 + 28\,x^4 + 2500 \tag{28}$$

```
> alias(theta=RootOf(f_min,x));
```

$$y1, y2, \theta \tag{29}$$

```
> evala(Factor(f_min,theta));
```

$$\left(\frac{1}{60}\,\theta^5 - \frac{11}{30}\,\theta + x\right)\left(x + \frac{1}{80}\,\theta^5 + \frac{39}{40}\,\theta\right)\left(-\frac{1}{60}\,\theta^5 + \frac{11}{30}\,\theta + x\right)\left(-\frac{1}{80}\,\theta^5 - \frac{39}{40}\,\theta + x\right)\left(\frac{1}{48}\,\theta^5 + \frac{7}{24}\,\theta + x\right)\left(-\frac{1}{48}\,\theta^5 - \frac{7}{24}\,\theta + x\right)(x + \theta)\,(x - \theta) \tag{30}$$

```
> ?
```

$$`?` \tag{31}$$

```
>
>
```